БОРЬБА С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ: ВЧЕРА, СЕГОДНЯ, ЗАВТРА*

Е.В. ЧАНОВ, председатель общественного объединения «Фонд ветеранов специальных подразделений «АСА»»

В статье анализируются вопросы, посвященные компьютерной преступности и борьбе с ней. Приводится краткий экскурс по созданию специальных международных органов противодействия данному негативному явлению. Подробно рассказывается о зарождении киберпреступности, большое внимание уделяется сотрудничеству отечественных и зарубежных спецслужб по борьбе с преступлениями в сфере высоких технологий. Подчеркивается общественная опасность глобализации компьютерной преступности, дается определение такого понятия, как кибертерроризм.

В XXI век – век информации и новых, доселе неизвестных, технологий – трудно найти какую-либо область жизни общества, где бы не использовались современные способы обработки и передачи информации. Однако подобные реалии не только развивают наше общество, но и создают условия, в немалой степени облегчающие осуществление преступных планов. Организованные преступные группы максимально используют возможности новых информационных технологий как для подготовки и совершения преступлений, так и для их сокрытия.

Еще 10–15 лет назад в Республике Беларусь этой проблемы, казалось, вообще не существовало. Не было ни самих киберпреступников, ни соответствующей законодательной базы. С приобретением независимости наша страна получила доступ к технологическим новшествам. Произошел своеобразный обмен: из бывшего СССР «утекали мозги», взамен наши знания обогащались тем бесценным высокотехнологическим опытом стран рыночной экономики, которого мы были лишены. Но к новым технологиям прилагался достаточно разнообразный «набор» совершенно новых, неизвестных ранее, преступлений. Кроме преступных деяний, где компьютерная техника была лишь средством или объектом преступления, появились совершенно специфические преступления, где объектом преступления стала информация, размещенная и на персональных компьютерах, и на компьютерах, соединенных как в локальную, так и глобальную информационные сети. Эти виды преступлений вошли в отдельный раздел Уголовного кодекса Республики Беларусь «Преступления против информационной безопасности».

Одна из главных особенностей – возможный значительный разрыв как в пространстве, так и во времени между действиями преступника и совершаемым им преступлением. Другая особенность, которая значительно усиливает первую, – полное отсутствие административно-территориальных границ в электронном пространстве и почти полная бесконтрольность прохождения информации. Копирование информации при несанкционированном доступе, как правило, не влечет изменение и изъятие самой информации и проходит незаметно. Это, в свою очередь, позволяет причислить преступления против информационной безопасности к латентным преступлениям, где не только раскрытие, но и сама его регистрация представляется сложной. По мнению зарубежных специалистов, совокупные материальные потери от компьютерных преступлений сопоставимы с потерями государства от преступлений в сфере налогового законодательства, торговли наркотиками, оружием и «живым» товаром, вместе взятыми.

По сведениям начальника отделения Интерпола в России С.И. Лашина, ежегодные потери только делового сектора США от несанкционированного проникновения в информационные базы данных составляют от 150 до 300 млрд долларов. Если усилия компьютерных преступников будут направлены на взлом баз данных систем, обслуживающих оборону и атомную энергетику, под угрозой окажется национальная безопасность любого государства. Может возникнуть опасность крупной техногенной катастрофы или даже войны. Специалисты по борьбе с международным терроризмом обеспокоены возможностью того, что террористические группировки могут прибегнуть к таким действиям. Они предупреждают, что компьютеры могут быть использованы для нанесения серьезного удара по критически важным объектам инфраструктуры, что может привести к значительным катастрофическим последствиям. Возможность глобализации, создание

* Статья поступила в редакцию 2 февраля 2007 года.

транснациональных преступных объединений также вселяет крайнюю тревогу.

Развитые страны еще в начале 90-х годов начали координировать свои усилия по противодействию преступности в области информационных технологий. Состоявшаяся в 1990 году XIX Европейская региональная конференция Интерпола приняла решение о создании специальной рабочей группы по компьютерной преступности с целью изучения основных тенденций ее развития. Рабочая группа начала свою деятельность в 1991 году при Европейском комитете Интерпола в Лионе (Франция). В ее состав вошли эксперты из восьми европейских стран и представитель генерального секретариата Интерпола.

Первоочередными задачами, поставленными перед рабочей группой на начальном этапе, стали:

- анализ проходящей через Интерпол информации о фактах компьютерных преступлений в странах-членах организации;
- организация и проведение ежегодных учебных курсов для сотрудников правоохранительных органов европейских стран;
- разработка и публикация сборника «Компьютеры и преступность», предназначенного для практического использования специализированными подразделениями, с описанием основной методологии и толкованием терминов, адресами национальных координационных центров в различных странах и другой необходимой информацией;
- проектирование модели стандартизированной формы сообщения о компьютерном преступлении;
- реализация кодификатора;
- организация и проведение тематических международных конференций Интерпола.

В апреле 1995 года в штаб-квартире генерального секретариата Интерпола в Лионе была проведена 1-я международная конференция по вопросам координации усилий. Участники пришли к выводу о необходимости создания национальных координационных центров по борьбе с компьютерной преступностью, которые могли бы в будущем образовать международную систему «раннего предупреждения». В настоящее время такие центры созданы более чем в 20 странах мира.

2-я конференция, состоявшаяся в мае 1996 года, приняла резолюцию о создании региональных рабочих групп по компьютерной преступности в Азиатско-Тихоокеанском регионе и Соединенных Штатах Америки. Кроме того, предусмотрено создание координационного комитета при генеральном секретариате Интерпола для регулирования деятельности всех перечисленных подразделений. Тогда же эта группа была переименована в Европейскую рабочую группу по преступлениям в сфере информационных технологий. Были определены три приоритетных направления ее деятельности: Интернет – изучение вопросов правового и полицейского характера; разработка рекомендаций по пресечению хищений, совершаемых с использованием электронных банковских платежных средств; способы предотвращения мошенничества, совершаемого с использованием средств связи и телекоммуникаций.

Весьма существенным недостатком в деятельности белорусских правоохранительных органов явилось отсутствие специалистов по борьбе с так называемой «беловоротничковой» преступностью, толчком к распространению которой послужило развитие компьютерных технологий. Для специалистов, занимающихся борьбой с компьютерной преступностью, стали проводиться учебные курсы. Лекции читали эксперты научно-исследовательских институтов и университетов, а также практические работники правоохранительных органов европейских стран. На базе учебных центров Великобритании, Германии, Португалии и Швейцарии проведено восемь выпусков [1, с.107]. В настоящее время все крупные полицейские учебные заведения развитых стран имеют специализированные факультеты или курсы.

В Беларуси первое «высокотехнологическое» преступление было зарегистрировано 20 ноября 1998 года. Им стало внедрение в компьютеры крупнейшего минского сервис-провайдера вредоносной троянской программы под названием «Back Orifice», что позволило преступнику осуществить несанкционированный доступ к сетевым реквизитам пользователей сети Интернет. Несмотря на то, что злоумышленник был изобличен, к уголовной ответственности его привлечь не удалось – отсутствовала соответствующая статья Уголовного кодекса.

С учетом этого преступления, а также ряда других имеющихся на тот момент правонарушений в сфере электронной информации, в связи со вступлением в действие с 1 января 2001 года нового УК, предусматривающего ответственность за совершение подобных преступлений, и благодаря изучению опыта своих коллег из стран ближнего и дальнего зарубежья в феврале 2001 года в структуре криминальной милиции МВД было создано управление оперативно-организационной работы. В него вошло специализированное отделение по раскрытию преступлений в сфере высоких технологий.

Сегодня Управление по раскрытию преступлений в сфере высоких технологий МВД Республики Беларусь (УРПСВТ) является высокопрофессиональным, самостоятельным оперативно-розыскным подразделением, непосредственно подчиненному начальнику главного управления криминальной милиции. Несмотря на то, что со времени создания прошло всего 6 лет, управление показало себя «грозой» киберпреступников. Если за период 1998–2000 годов было возбуждено всего тр

уголовных дела, связанных с использованием высоких технологий, то с 2001 по 2005 год – 1813. Только за 2006 год было выявлено 847 преступлений, совершенных с использованием компьютерной техники, программных средств и сети Интернет, из них – 334 преступления против информационной безопасности.

Большой вклад УРПСВТ внесло и в борьбу с международной компьютерной преступностью. 2006 год дал впечатляющие результаты:

• участие в известной международной операции по борьбе с детской порнографией Operation Falcon («Сокол»), следствием которой явилось задержание организаторов во Франции и Испании;

• раскрытие большой международной группы интернет-мошенников, состоящей из граждан России, Молдовы и Беларуси и причинившей убытки компаниям и частным лицам США, Австралии, Новой Зеландии и других стран на сотни тысяч долларов США;

• изобличение и задержание компьютерных взломщиков канадских интернет-компаний;

• поимка совместно с российскими коллегами порнодельцов из Пскова;

• совместная работа с Национальным комитетом по борьбе с преступностью в сфере высоких технологий Великобритании, результатом которой стала поимка мошенников, писавших так называемые «нигерийские письма», выманивавшие деньги у доверчивых граждан;

• участие в международной специальной операции по борьбе с детской порнографией в сети Интернет под кодовым названием «Невинные картинки» (Innocent Images Task Force). В результате задержан 61 распространитель, выявлено 1200 web-сайтов [2].

Глобализация киберпреступности рассматривается сегодня международным сообществом как одна из важнейших и актуальнейших проблем современности. В 2000 году принята Хартия глобального информационного сообщества, а 23 ноября 2001 года странами, входящими в Совет Европы, подписана Конвенция о борьбе с киберпреступностью, в преамбуле которой говорится о важности консолидации усилий всего мирового сообщества перед опасностью международной компьютерной преступности. В феврале 2003 года в Атланте (США) проведен Первый международный саммит по проблемам киберпреступности. Прогнозы специалистов-участников саммита были далеко не радужными – международная киберпреступность растет в геометрической прогрессии; законодательство и меры противодействия самых развитых стран не позволяют справиться с этим явлением. Сегодня 100 стран (в т.ч. 60% членов Интерпола) не имеют даже адекватной законодательной базы для борьбы с киберпреступлениями.

Особого внимания и изучения заслуживает такое новое для нас явление, как кибертерроризм. Под *кибертерроризмом* понимается преднамеренная, мотивированная атака на информацию, обрабатываемую компьютером, компьютерную систему и сети, которая создает опасность для жизни и здоровья людей или наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта.

Как и при обычном терроризме политическая составляющая кибертерроризма всегда стоит на первом месте. Поэтому не случайно основными мишенями стали развитые страны и в первую очередь США (около 40% всех кибератак), в ответ на свою политику монополярного мира, войны в Ираке и т.д. Достаточно вспомнить печально известный «червь» VBS/Nedal (Laden – наоборот), который (кроме разрушения рабочих программ) воспроизводил текст, призывающий стереть с лица земли Израиль и США. Исламские экстремисты даже ввели понятие «электронного джихада», заявляя, что ими настойчиво изучаются современные достижения в области высоких технологий, чтобы превратить их в оружие против того, кто их и создал, – США и другие развитые страны.

Экономические потери от подобных действий огромны. По оценке специалистов американской группы «Компьютер экономик», только один вирус «I love you» за первые пять дней с момента своего появления нанес ущерб в размере нескольких миллиардов долларов. Известный вирус Slammer прекратил работу сети Интернета в Корее и Японии на несколько часов и заразил как минимум 80 тысяч компьютеров [3]. В ноябре 1994 года в компаниях «Дженерал Электрик» и «Нешнл Бродкастинг Корпорэйшн» на несколько часов была нарушена работа внутренних информационных сетей, что привело к колоссальным убыткам. Ответственность за эту акцию взяла на себя организация «Фронт освобождения интернет», объявив «кибервойну» данным компаниям [4].

Особо опасными такие действия становятся тогда, когда преступник получает доступ к автоматизированным банкам данных, обслуживающим системы национальной обороны и атомной энергетики. Яркая иллюстрация этому – пример с группой «хакеров» (одержимых программистов) «Банда 414», возглавляемой Нилом Патриком. После того как ФБР напало на след этой группы «электронных диверсантов», оказалось, что ее члены обеспечили себе несанкционированный доступ к более чем 50 автоматизированным банкам данных, включая Лос-Аламосскую ядерную лабораторию, крупный раковый центр и другие жизненно важные объекты США [5, с.45].

Для информационных актов характерны следующие инструменты их совершения:

• различные виды атак, позволяющие проникнуть в атакуемую сеть или перехватить управление сетью;

• компьютерные вирусы, в том числе сетевые (черви), модифицирующие и уничтожающие информацию или блокирующие работу вычислительных систем;

• логические бомбы – наборы команд, которые внедряются в программу и срабатывают при определенных условиях (например, по истечении определенного отрезка времени);

• «троянские кони», позволяющие выполнять определенные действия без ведома хозяина зараженной системы;

• средства подавления информационного обмена в сетях.

Сложность в предупреждении кибертерроризма заключается в ряде характеризующих его аспектов:

• латентность (скрытность);

• трансконтинентальность (трансграничность);

• информация, информационные ресурсы, информационная техника могут выступать целью преступных посягательств и орудием преступления;

• легкость уничтожения и изменения компьютерной информации (следов преступления).

Спецслужбы западных стран оценивают реальную угрозу кибертерроризма и разрабатывают превентивные меры. Разрабатываются несколько возможных сценариев развития событий, в частности, возможной атаки на компьютерные системы фондовых бирж.

Последствия компьютерных вторжений, вероятнее всего, могут быть двух типов: вторжение в данные и вторжение в системы управления и контроля.

1. Вторжение в данные – это нападения на сайты, сетевые компьютеры, системы платежей и связанные с этим базы данных.

2. Вторжение в системы управления и контроля будет направлено на отключение или разрушение государственной или корпоративной инфраструктуры.

Последствиями вторжения в данные будут банкротство коммерческих структур, воровство, уничтожение важной деловой информации, потеря интеллектуальной собственности, снижение репутации и (или) снижения цены акции. Вторжение в системы управления и контроля представляет большую опасность – сбой работы коммуникаций, транспорта, передачи данных, финансовых систем оплаты и другие [6].

Несмотря на то, что современное законодательство Республики Беларусь и ее правоохранительные органы обеспечивают адекватную реакцию на компьютерные преступления, «битва» за информационную безопасность только начинается. Перед белорусским государством и теми, кому поручена его безопасность, соблюдение закона, стоит задача работать на опережение новых криминальных проявлений, и в первую очередь – компьютерных преступлений. Сделать это можно, лишь объединив усилия всех заинтересованных ведомств, как в масштабе отдельно взятого государства, так и мирового сообщества в целом.

ЛИТЕРАТУРА

1. Лашин, С.И. Преступность в области информационных технологий / С.И. Лашин // Технологии и средства связи, 1997. №1. С. 107–108.

2. Официальный интернет-портал МВД Республики Беларусь / http://mvd.gov.by/

3. Номоконов, В.А. Актуальные проблемы борьбы киберпреступностью / В.А. Номоконов // Сборник научных трудов международной конференции «Информационные технологии и безопасность». Выпуск 3. Киев: Национальная академия наук Украины, 2003. С. 104–110.

4. Голубев, В.А. «Кибертерроризм» – миф или реальность? / http://www.crime-research.org.

5. Федоров, В.В. Компьютерные преступления: выявление, расследование и профилактика / В.В. Федоров // Законность, 1994. №6. С. 44–47.

6. Голубев, В.А. Проблемы борьбы с кибертерроризмом в современных условиях / http://www.crime-research.org.

SUMMARY

The problems concerned with computer fraud and fighting computer fraud are analyzed in the article. A short excursus into creating special international organizations for opposing this negative phenomenon is given. The story about the origin of cyber crime is told in details, a lot of attention is paid to the cooperation of internal and foreign special services specialized in fighting crimes in the sphere of high-tech. The public danger of the globalization of computer crimes is emphasized and the definition of the concept of cyber terrorism is given.