УДК 343.3/7 (575.2) (04)

НЕКОТОРЫЕ АСПЕКТЫ КИБЕРПРЕСТУПНОСТИ И СПОСОБЫ БОРЬБЫ С НЕЙ

И.В. Коваль

Рассматриваются вопросы, связанные с классификацией киберпреступности, методикой борьбы с ней, а также анализируется законодательство разных стран по данной проблематике.

Ключевые слова: киберпреступность; компьютерные технологии; преступления в сфере IT- технологий; Интернет; меры противодействия.

Преступления в сфере IT-технологий чрезвычайно разносторонние и сложные явления. Объектами таких преступных действий могут быть как сами технические средства (компьютеры и периферийные устройства) так и материальные объекты или программное обеспечение и базы данных, для которых технические средства являются окружением. Персональный компьютер может выступать как предмет посягательства или как инструмент правонарушения.

Начальник Управления безопасности Минсвязи России В. Оранжереев обратил внимание собравшихся на недавнее ЧП в Москве, когда запущенный неизвестным хакером вирус на несколько дней отключил электронную систему оплаты коммунальных платежей в Северо-Западном округе столицы. В результате, если в один из компьютеров сети попадает вирус, пресечь его распространение становится крайне сложно. Интересно, что бы произошло в случае, если бы аналогичный вирус проник в какую-нибудь федеральную сеть? Судя по старту федеральной целевой программы (ФПЦ) "Электронная Россия", которая начиная со 2004 г. вынимает из федерального бюджета по 7,5−8 млрд. рублей в год, вопрос этот отнюдь не праздный. По сравнению с аналогичными программами в США "Электронная Россия" куда более уязвима с точки зрения вероятной виртуальной киберкатастрофы. Когда компьютеры предприятий, финансовых и торговых организаций, больниц и школ, аэропортов и автовокзалов через Интернет свяжутся в единую сеть, мировые кибертеррористы ополчатся против них столь же энергично, как сейчас − против американских организаций.

История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона в 1978 году. Принятый закон назывался "Computer crime act of 1978"[1] и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства.

Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения киберпреступлений[2]. Отечественное и российское законодательство движется в этом направлении очень медленно.

Виды киберпреступности весьма разнообразны. Это и несанкционированный доступ к информации, хранящейся в компьютере, и ввод в программное обеспечение "логических загадок (бомб)", которые срабатывают при выполнении определенных условий и частично или полностью выводят из строя компьютерную систему, и разработка и распространение компьютерных вирусов, и хищение компьютерной информации.

Компьютерное преступление может произойти также из-за небрежности в разработке, изготовлении и эксплуатации программно-вычислительных комплексов или из-за подделки компьютерной информации.

[1] http://www.nezachetovnet.ru/free/kriminalogiya

[2] *Крылова В.В.* Информационные компьютерные преступления. М.: Инфра-М – Норма, 1997. С. 21.

В настоящее время все меры противодействия компьютерным преступлениям можно подразделить на технические, организационные и правовые[1]. К техническим мерам можно отнести защиту от несанкционированного доступа к компьютерной системе, резервирование важных компьютерных систем, принятие конструктивных мер защиты от хищений и диверсий, обеспечение резервным электропитанием, разработку и реализацию специальных программных и аппаратных комплексов безопасности.

К организационным мерам относятся: охрана компьютерных систем, подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра после выхода его из строя, обеспечение обслуживания вычислительного центра посторонней организацией или лицами, не заинтересованными в сокрытии фактов нарушения работы центра, универсальность средств защиты от всех пользователей (включая высшее руководство), возложение ответственности на лиц, которые должны обеспечить безопасность центра, выбор места расположения центра и т.п. Решению этих вопросов посвящено большое количество научных исследований и технических разработок.

К правовым мерам следует отнести разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного, уголовно-процессуального законодательства. К правовым мерам относятся также вопросы общественного контроля за разработчиками компьютерных систем и принятие соответствующих международных норм. Отечественное законодательство также встало на путь борьбы с компьютерной преступностью[2]. Поэтому весьма важно расширить правовую и законодательную информированность специалистов и должностных лиц, заинтересованных в борьбе с киберпеступлениями.

Преступления в сфере компьютерных технологий не имеют территориальных ограничений. Их предупреждение и пресечение требует принятия совместных мер и решений со стороны всех заинтересованных государств. И одним из первых документов для стран-участниц СНГ, направленных на борьбу с кибепреступлениями, стало Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, подписанное всеми странами СНГ в Минске 1 июня 2001 года[3].

В странах СНГ принято Соглашение по борьбе с киберпреступлениями, которое определяет характер преступлений и ответственность за правонарушения:

а) преступление в сфере компьютерной информации − уголовно наказуемое деяние, предметом посягательства которого является компьютерная информация;

б) компьютерная информация − информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи;

в) вредоносная программа − созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети;

г) неправомерный доступ − несанкционированное обращение к компьютерной информации[4].

Немаловажным является и то, что Соглашением обобщены уголовно-наказуемые деяния в сфере компьютерной информации, совершенные умышленно:

а) осуществление неправомерного доступа к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию, либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети;

б) создание, использование или распространение вредоносных программ;

в) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети, повлекшее уничтожение, блокирование или модификацию охраняемой законом компьютерной системе в силу должностных обязанностей;

г) незаконное использование программ для ЭВМ и баз данных, являющихся объектами авторского права, а равно присвоение авторства,

---

[1] *Айков Д., Сейгер К., Фонсторх У.* Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями / Пер. с англ. М., 1999.

[2] УК КР. Гл. 28. Преступления в сфере компьютерной информации.

[3] *Вехов В.Б.* Компьютерные преступления. М.: Право и Закон, 1996.

[4] http://medialaw.asia/document/2463-2468

если это деяние причинило существенный ущерб.

Анализируя законодательство стран СНГ можно сделать вывод, что в законодательстве всех государств-участников СНГ предусмотрена уголовная ответственность за совершение перечисленных выше уголовно-наказуемых деяний. Более того, в некоторых странах, таких как Армения, предусмотрено более узкое деление перечисленных видов деяний: среди них "Компьютерный саботаж" или "Хищение, совершенное с использованием компьютерной техники" (Статья 181, УК Республики Армения)[1].

На практике количество возбужденных уголовных дел по киберпреступлениям не так велико ввиду сложности обнаружения злоумышленников и сбора доказательственной базы. Однако компьютерных преступлений гораздо больше, нежели статей, предусматривающих уголовную ответственность за киберпреступления. На наш взгляд, более детального исследования требуют преступления, совершенные посредством сети Интернет, в результате чего будут сформированы нормы для уголовного и уголовно-процессуального законодательства, которые будут учитывать специфику совершения киберпреступлений.

Сегодня, по оценкам специалистов, объем рынка профессиональных услуг в области компьютерных преступлений составляет 1 млрд. долларов в год, и при этом он находится в стадии интенсивного роста[2]. Наибольшим рискам подвергаются крупные организации, прежде всего – банки и вертикально-интегрированные холдинги. В перспективе в зону риска также попадут многочисленные предприятия среднего бизнеса – и как непосредственные объекты преступлений, и как "транзитные площадки" для криминальных действий в отношении более крупных компаний. Соответственно возрастет число таких компьютерных преступлений, как мошенничество в системах Интернет-банкинга, нарушение работы информационных систем и атаки, направленные против конкретных брендов в сети Интернет.

Бороться с компьютерными преступлениями можно разными способами, в частности, создавать организации для борьбы с киберпреступлениями. Основное функциональное подразделение компании − отдел расследований – состоит из трех групп: группы расследований, которая занимается собственно расследованием инцидентов; группы мониторинга и реагирования, которая может подсказать в момент инцидента как минимизировать риски и как правильно собрать юридически значимые доказательства; группы аналитиков, которая годами собирает данные по расследованиям незаконной деятельности в Интернете и создает по ним базу данных.

Второе функциональное подразделение – лаборатория компьютерной криминалистики; третье – отдел безопасности, который следит за тем, чтобы сотрудники компании не нарушали законов в ходе расследований, поскольку эта работа не должна носить характер оперативно-розыскной деятельности, а также за тем, чтобы сотрудники не начинали общаться с киберпреступниками; четвертое – юридический отдел, который занимается рассмотрением дел в судах и МВД; пятое – отдел, который обеспечивает постинцидентный консалтинг. Компетенции и наработанные информационные базы, приемы и технологии позволяют компании раскрывать сложные криминальные схемы, зачастую объединяющие киберпреступные сообщества разных стран.

В 2002 г. было создано Бюро специальных технических мероприятий (БСТМ) при МВД России. В настоящее время эти подразделения называются Отделы "К" (по борьбе с компьютерными преступлениями). В них сохранены профильные отделения по трем направлениям борьбы с компьютерными преступлениями:

1. Отделение по борьбе с преступлениями в сфере компьютерной информации.

2. Отделение по борьбе с преступлениями в сфере телекоммуникаций.

3. Отделение по борьбе с незаконным оборотом радиоэлектронных (РЭС) и специальных технических средств (СТС).

В системе МВД России функционируют два профильных научно-практических учреждения, обеспечивающих работу по борьбе с компьютерными преступлениями:

1. Научно-исследовательский институт МВД России (НИИ МВД России).

2. Научно-исследовательский институт специальной техники МВД России (НИИСТ МВД России)[3].

Конечно, в этом направлении должны работать многие компании (возможно и лицензированные частные компании) – без этого за киберпреступниками не угнаться. Самое сложное в этой

[1] УК Республики Армения.

[2] http://www.nezachetovnet.ru/free/kriminalogiya

[3] http://www.cyberpol.ru/cybercops.shtml#p_01

работе – добиться понимания законодательных органов. Разработка проблемы компьютерной преступности и поиск методов борьбы с нею всего лишь дело времени и опыта. И российские и кыргызские криминалисты внесут в это свой вклад.

Отдел “К” УВД РФ по ПК предлагает:

Пользователям: применять только лицензионное программное обеспечение, включая лучшие антивирусные программы, “сетевые экраны”, защищённые Интернет-браузеры и почтовые клиенты, средства криптографии. Данные вопросы широко освещены в сети Интернет и некоторых компьютерных периодических изданиях. Читайте и учитесь!

Организациям: дополнительно к указанным выше мерам, назначать лиц, ответственных за компьютерную безопасность.

Провайдерам: при заключении договоров вручать абоненту памятку с рекомендациями по компьютерной безопасности. Предлагать абоненту тот вид доступа, который обеспечит наибольшую безопасность решения им поставленных задач.

При возникновении компьютерного инцидента: принять меры по сохранению информации на жёстких дисках ПК. Зарисовать (как есть) конфигурацию локальной сети, указав для её хостов соответствующие сетевые настройки, включая MAC-адреса сетевого оборудования. Указать на этой схеме, какое сетевое оборудование и ПО используется на данных хостах (отметить наличие лицензий), кто из сотрудников использует хост. Обнаруженное вредоносное ПО сохранить на CD, отметив, где оно обнаружено, при каких обстоятельствах и кем могло быть внесено в сеть. Со всем этим следует обратиться в орган внутренних дел, взяв с собой договор с провайдером и приложение к договору, содержащее технические параметры доступа в Интернет. При обращении в ОВД, кроме лица, заключившего договор, необходимо присутствие системного администратора (для организаций).

На сайте МВД Кыргызской республики на запрос отдела “К”, получен ответ: Всего найдено 0 записей. Возможно создание такого отдела в Кыргызстане это ближайшее будущее.