Объединенный институт проблем информатики
Национальной академии наук Беларуси

VIII Международная конференция

РАЗВИТИЕ ИНФОРМАТИЗАЦИИ И ГОСУДАРСТВЕННОЙ СИСТЕМЫ НАУЧНО-ТЕХНИЧЕСКОЙ ИНФОРМАЦИИ

РИНТИ-2009

16 ноября 2009 года, Минск

Доклады

Минск
ОИПИ НАН Беларуси
2009

УДК 004

ПРАВОВАЯ ЗАЩИТА ОТ КИБЕРАТАК И ДЕЙСТВИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

М.С. Абламейко, С.В. Абламейко
Белорусский государственный университет, Минск

Проводится анализ имеющихся на сегодняшний день международных правовых документов, регулирующих действия стран при кибератаках. Показывается, что имеющиеся механизмы недостаточны для защиты и правовой оценки последствий от кибератак. Отмечается, что Республика Беларусь начала предпринимать меры по участию в выработке правовых мер, в том числе международного характера, по защите от киберугроз.

Введение

Развитие и все более широкое распространение информационных и телекоммуникационных технологий, обеспечивающих эффективное пользование информационными ресурсами, определило необходимость правовой оценки ситуации и разработки организационно-правовых механизмов пресечения общественно опасного поведения в данной области – киберпреступности. Преступные проявления в сфере высоких технологий, так называемая киберпреступность, свойственны всем государствам, которые в силу научно-технического прогресса перешли на новую, инновационную ступень своего развития.

После первого этапа простого распространения вирусов хакеры начали вести направленные кибератаки всевозможных компьютерных систем с целью завладения секретной информацией и денежными средствами. Таким образом, человечество постепенно перемещается в эпоху кибервойн (войн в киберпространстве), которые по своим последствиям могут быть не менее разрушительными, чем обычные войны.

Лидером по количеству кибератак являются США, на счету которых 35,4 % от мирового коэффициента киберпреступлений за второе полугодие 2002 г. Второе место в списке кибернарушений занимает Южная Корея – 12,8 %, за ней Китай – 6,9 %, Германия – 6,7 %; Франция – 4 %. Великобритания занимает 10 место, где совершается 2,2 % от всего коэффициента кибератак. Самыми распространенными среди них являются: программные вирусы, саморазмножающиеся компьютерные вирусы и другие формы сбоев программного кода. Тот факт, что США лидируют в этом списке, вполне закономерен, так как здесь по сравнению с другими странами наблюдается наибольшее число (около половины) пользователей. Что касается относительного уровня, т. е. количества кибератак на тысячу интернет-пользователей, то во втором полугодии 2002 г. Южная Корея (23,7 % от общего числа) оставила далеко позади все другие страны. Второй в списке среди стран с более чем одним миллионом пользователей следует Польша (18,4 %), за ней Чехия (14,2 %), Франция (14,2 %) и Тайвань (14 %).

В России происходит стремительный рост компьютерной преступности – с 33 преступлений в 1997 г. до 3 700 в 2002 г. В Беларуси произошел рост преступлений против информационной безопасности с 119 в 2003 г. до 1 614 в 2008 г. (130 – в 2004 г., 272 – в 2006 г., 996 – в 2007 г.).

Проанализировав динамику роста киберпреступлений, можно сделать вывод, что уголовно-правовая борьба с киберпреступностью – это глобальная проблема. Для эффективной борьбы с киберпреступлениями необходимо не только принятие соответствующих уголовно-правовых норм на национальном уровне, но и выработка единых международных стандартов, так как данный вид преступности носит трансграничный и межго-

сударственный характер. Также важно, чтобы национальное законодательство Республики Беларусь в данном вопросе соответствовало международным нормам и стандартам.

В докладе рассматриваются правовые механизмы противодействия киберпреступности, которые существуют в настоящее время в мире, анализируются действия Республики Беларусь по рассматриваемой проблеме.

1. Основные понятия

Под киберпреступностью понимается совокупность преступлений, совершаемых в киберпространстве с помощью или посредством компьютерных систем либо компьютерных сетей, а также иных средств доступа к киберпространству, в рамках компьютерных систем или сетей, против компьютерных систем, компьютерных сетей и компьютерных данных.

Согласно рекомендациям экспертов ООН термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети, против компьютерной системы или сети. В принципе оно охватывает любое преступление, которое может быть совершено в электронной среде. Иначе говоря, к киберпреступлениям относятся такие общественно опасные деяния, которые совершаются с использованием средств компьютерной техники в отношении информации, обрабатываемой и используемой в Интернете.

Из данного определения следует понятие самого деяния. Киберпреступление – это виновно совершенное общественно опасное и уголовно наказуемое вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также иные противоправные общественно опасные деяния, совершенные с помощью или посредством компьютеров, компьютерных сетей и программ, иных устройств доступа к моделируемому с помощью компьютера информационному пространству.

2. Документы и мероприятия ООН для защиты от кибератак

Как известно, одним из основополагающих документов, регулирующим правовое взаимодействие стран, является Хартия ООН. Данный документ был принят более 50 лет назад и конечно не предусматривал в то время правовую защиту от кибератак. Тем не менее многие государства стараются применить данный документ для правовой оценки кибернападений. Наиболее подходящими являются статьи 51 и 41. Так, статья 51 гласит, что никто не может запретить нации или группе наций организовать самозащиту, если произошла вооруженная атака. Однако здесь возникает вопрос: является ли кибератака вооруженной атакой? Даже если установлено, что атака произошла из подразделений вооруженных сил?

Бангкокская декларация, которая стала результатом деятельности XI Конгресса ООН по предупреждению преступности и уголовному правосудию, также свидетельствует об актуальности проблемы киберпреступности. В декларации отмечается, что в период глобализации быстрое развитие информационных технологий и новых систем телекоммуникаций и компьютерных сетей сопровождается злоупотреблением этими технологиями в преступных целях, а также подчеркивается необходимость разработки национальных мер и развития международного сотрудничества по противодействию киберпреступности.

Основной структурой ООН, работающей в сфере информационных технологий, является Международный союз телекоммуникаций, который в мае 2007 г. принял Гло-

бальную повестку по кибербезопасности. Она является большим комплексом международных мероприятий, объединяет всех желающих для достижения общих целей по киберстабильности. Затем была создана группа высококвалифицированных экспертов, включающая около 100 самых известных ученых из разных стран мира. Однако США открыто критикуют Международный союз телекоммуникаций за Глобальную повестку по кибербезопасности и отказались его поддержать. Развивая данное направление, Международный союз телекоммуникаций в 2009 г. выступил с инициативой создать международный Протокол против киберугроз.

3. Документы и действия НАТО, Совета Европы и ОДКБ по защите от кибератак

В Североатлантическом договоре НАТО используются такие термины, как «вооруженная атака», «территориальная целостность», «политическая независимость» и т. д. Термины «самозащита», «помощь», «коллективная помощь» используются только в контексте вооруженного нападения.

Статья 12 Североатлантического договора позволяет странам НАТО проводить совместные консультации по анализу договора, если имеются «факторы, угрожающие миру и стабильности». Эта статья может быть использована как механизм, при помощи которого кибератаки, коллективная защита и гео-кибербезопасность могут рассматриваться странами НАТО.

После произошедших событий в 2007 г. министр обороны Эстонии Яак Аавиксоо отмечал в СМИ, что данный договор НАТО не может объяснять и помогать в случае кибернападений, и ни один министр обороны страны НАТО не будет квалифицировать кибератаку как военное нападение на его страну.

Совет Европы в 2001 г. принял Конвенцию о киберпреступности, которая предлагает различные способы для совместной правовой работы стран по оценке кибератак и мер по их отражению. Конвенция предусматривает принятие сторонами законодательных и иных мер, которые позволят квалифицировать в качестве преступления такие деяния, как противозаконный доступ к компьютерной системе, противозаконный перехват данных, воздействие на данные и на функционирование системы, противозаконное использование устройств, подлог и мошенничество с использованием компьютерных технологий, правонарушения, связанные с детской порнографией, правонарушения, связанные с нарушением авторского права и смежных прав, а также покушение, соучастие или подстрекательство к совершению указанных преступлений (статьи 2-11 Конвенции). Данная Конвенция вступила в силу 01.07.2004 г. и является единственным имеющим обязательную силу международным инструментом в этой области.

В последние годы на заседаниях Организации договора коллективной безопасности (ОДКБ) регулярно стали рассматриваться вопросы, касающиеся кибербезопасности. Одним их последних мероприятий стало проведение 15.04.2009 г. на территории стран-членов ОДКБ широкомасштабной операции «Прокси» по противодействию киберкриминалу. Эта кампания направлена на выявление и пресечение в национальных сегментах Интернета информационных ресурсов криминального характера.

Россия является очень активной по предупреждению киберугроз. В 1998 г. она представила Резолюцию ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», определив основные понятия неавторизованных вторжений в компьютерные сети и предложив международные принципы защиты от кибернападений. В 1999 г. Резолюция включила военные угрозы, проистекающие от информационных и телекоммуникационных технологий. Такого типа ре-

золюции регулярно одобряются Генеральной Ассамблеей ООН, а США регулярно голосуют против них.

Российское МВД ежегодно проводит мероприятия под условным названием «Сеть» уже на протяжении 10 лет. Только в прошлом году в ходе такой операции была приостановлена деятельность 610 деструктивных интернет-ресурсов, возбуждено 270 уголовных дел, выявлено 325 преступлений.

4. Предложения мирового научного сообщества по обеспечению киберстабильности

Ученые развитых стран были одними из первых, кто стал обращать внимание на всевозрастающую опасность киберугроз. С начала 90-х гг. XX в. каждый год возрастает количество крупных международных форумов, на которых все чаще говорится о необходимости принятия действенных мер по правовой защите от кибератак.

Всемирная федерация ученых, одно из крупнейших в мире объединений, в 2001 г. создала специальную секцию по информационной безопасности и регулярно рассматривает вопросы, связанные с внешними воздействиями на компьютерные сети, публикует материалы, показывающие важность проблемы и пути ее разрешения. На своем последнем заседании в августе 2009 г. в итальянском городе Эриче федерация приняла специальную Декларацию о принципах киберстабильности и кибермира. В ней говорится о том, какие меры должны принять правительства стран, что необходимо сделать интернет-провайдерам, пользователям, чтобы гарантировать свободный и безопасный доступ к мировым интернет-ресурсам. Все государства должны активно участвовать в усилиях ООН, чтобы обеспечить киберстабильность в мире.

Всемирная федерация ученых в 2009 г. разработала список самых важных проблем в сфере кибербезопасности, в котором приведены самые важные юридические, политические и технические проблемы, на решении которых необходимо сконцентрироваться в ближайшее время.

5. Действия Республики Беларусь и Союзного государства

СНГ и Союзное государство предпринимают совместные шаги по защите от киберугроз. Например, в июне 1999 г. была принята концепция информационной безопасности стран СНГ, и в списке источников угроз этой безопасности первым пунктом названа «государственная политика ряда зарубежных стран, направленная на осуществление глобального мониторинга политических, экономических, военных, экологических и других процессов в целях получения односторонних преимуществ».

В декабре 1999 г. была одобрена программа действий России и Беларуси по реализации положений договора о создании Союзного государства. В разделе о совместной деятельности спецслужб появился пункт: «Осуществляются мероприятия против негативного информационного воздействия на государственные органы, общественные организации и население Союзного государства, а также пресекаются любые попытки противоправной разведывательной деятельности специальных служб и организаций третьих стран…». В дальнейшем в целях обеспечения эффективной борьбы с преступлениями в сфере компьютерной информации 7.09.2001 г. был подписан Указ Президента Республики Беларусь № 475 «Об утверждении соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации».

За последние 10-15 лет в Республике Беларусь принималось немало серьезных мер по защите собственных компьютерных сетей от кибератак. Они рассматриваются и разрабатываются в государственных программах различного уровня. Имеются также и программы Союзного государства в сфере информационной безопасности. Одним из крупнейших форумов, где регулярно происходит обмен мнениями, является ежегодная научно-техническая конференция Союзного государства «Проблемы защиты информации». Уже 10 лет издается российско-белорусский научно-практический журнал «Управление защитой информации», в Беларуси издается сборник статей «Проблемы правовой информатизации». На юридическом факультете БГУ разработана и внедрена в учебный процесс программа «Правовая информатика».

В МВД Республики Беларусь создано и функционирует специальное подразделение по борьбе с киберпреступностью (по противодействию преступлений в сфере высоких технологий). В Уголовном кодексе Республики Беларусь в разделе XII «Преступления против информационной безопасности», глава 31 «Преступления против информационной безопасности» в статье 349 «Несанкционированный доступ к компьютерной информации» говорится о следующем:

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), повлекший по неосторожности оборудования либо причинение иного существенного вреда, – (абзац 1 части 1 статьи 349 в ред. Закона Республики Беларусь от 22.07.2003 № 227-З) наказывается штрафом или арестом на срок до шести месяцев.

2. Несанкционированный доступ к компьютерной информации, совершенный из корыстной или личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, (абзац 1 части 2 статьи 349 в ред. Закона Республики Беларусь от 22.07.2003 № 227-З) наказывается штрафом или лишением права занимать определенные должности, или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризированной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Сотрудниками подразделения раскрыто немало преступлений, связанных со взломом компьютерных сетей.

МВД активно участвует в выработке международных механизмов по предотвращению киберпреступности. Делегация МВД в марте 2009 г. приняла участие в Вене в рабочем совещании ОБСЕ по всеобъемлющему подходу к повышению кибербезопасности. Сотрудники правоохранительных органов стран Европы и США, представители ОБСЕ, Европейской Комиссии, Парламентской ассамблеи Совета Европы и другие эксперты в обозначенной сфере рассмотрели проблемы сотрудничества в вопросах защиты от кибератак в оборонном, банковском и энергетическом секторах, а также на государственные сайты. Особый акцент при этом был сделан на необходимость присоединения государств к Конвенции Совета Европы по кибербезопасности, подписание которой позволит выйти на более качественный уровень взаимодействия.

В Республике Беларусь до сих пор не отмечалось каких-либо массированных нападений на компьютерные сети. Одним из самых больших событий, нарушивших стабиль-

ность работы компьютерных сетей, стал в 2009 г. сбой в работе сети Национального процессингового центра, который привел к отказу от обслуживания большого количества банкоматов. Это произошло из-за вируса, однако учитывая размер происшествия и его последствия, Правительство Республики Беларусь поручило Министерству связи и информатизации совместно с заинтересованными разработать перечень мер по предотвращению сбоев в компьютерных сетях. Такой объемный документ был разработан и утвержден летом 2009 г. Первым заместителем Премьер-министра Республики Беларусь.

Заключение

Из проведенного анализа ясно, что ни Хартия ООН, ни Договор НАТО, ни какой-либо другой международный документ не предусматривал кибернападений на такие жизненно важные структуры стран, какими стали компьютерные сети, и не может напрямую быть использован применительно к появившимся новым вызовам XXI в. Очевидно, что настала чрезвычайная необходимость для разработки новых правовых механизмов защиты от массированных кибератак. Всем странам мирового сообщества необходимо предпринять решительные совместные шаги по недопущению кибернападений и правовой оценке их последствий.