К односторонним действиям относится создание национальной законодательной базы, предусматривающей уголовную ответственность за совершение преступлений, классифицируемых как «киберпреступления». Они также включают несанкционированные действия:

доступ к компьютерам и компьютерным системам;

изменение компьютерных данных;

перехват данных;

попытки отказать в законном доступе к компьютеру или компьютерной системе [1, с. 43].

Односторонние действия не могут быть панацеей при борьбе с киберпреступностью. Эффективное решение международных проблем в данной области невозможно без международного сотрудничества. Тем не менее в качестве основы или предпосылки к международному сотрудничеству, экстрадиции и взаимопомощи государства должны иметь возможность самостоятельно реагировать на киберпреступления.

Частичное сотрудничество. С момента, когда в государстве возникает законодательная база для борьбы с киберпреступностью, может возникнуть необходимость в установлении партнерских отношений в данной области со странами-соседями. Например, экстрадиция может быть распространена и на осужденных по статьям о киберпреступлениях. К ним относятся соглашения о сотрудничестве на рабочем уровне как формальные, так и неофициальные.

Всестороннее сотрудничество. Двустороннее сотрудничество может быть формой взаимной юридической помощи. Но в связи с тем, что проблема киберпреступности затрагивает практически все мировые государства, заключать двусторонние соглашения со всеми заинтересованными странами может быть довольно неэффективной формой сотрудничества. Поэтому необходимо искать многосторонние соглашения, возможно, на базе ООН. Всестороннее сотрудничество является выгодным, так как исключает чрезмерные сложности, возникающие при большом количестве двусторонних соглашений, а также способствует разрешению спорных вопросов, возникающих за счет разногласий в законодательствах между странами-партнерами. Более того оно вообще является базовым для международного правового сотрудничества в области борьбы с киберпреступностью.

Очевидной остается необходимость в многостороннем международном сотрудничестве, без которого эффективная борьба с киберпреступностью просто невозможна.

Экстратерриториальное регулирование станет проще, даже если территориальность останется критическим фактором криминального регулирования или преследования. Различные экстратерриториальные трудности и разногласия, имеющие место в настоящее время, которые связаны с уже слегка устаревшими концепциями суверенитета и юрисдикции, в ближайшем будущем исчезнут. Широкий спектр возможностей для граждан одной страны влиять на жизнь граждан других стран приводит к неизбежному

переосмыслению понятия «суверенитета». Важно также отметить, что концепция территориальности по-прежнему остается базовой.

Взаимное международное сотрудничество будет развиваться. Совместно с ослаблением «традиционных» сомнений в отношении экстратерриториального регулирования государства начнут самостоятельно способствовать взаимному международному сотрудничеству, что ни в коей мере не будет противоречить понятию «суверенитета», так как одним из его атрибутов является способность государства устанавливать отношения с другими государствами порой даже независимо от понятия территориальности [2, с. 166]. Для достижения положительных результатов требуется участие максимально возможного количества стран. Этот процесс, безусловно, займет немалое время. Если еще учесть разный уровень технического развития стран, то становится очевидным, что технологии неизбежно будут опережать законодательство.

1. Юдин О.К, Богуш В.М. Інформаційна безпека держави : навчал. посібник. Харків : Консум, 2005.

2. Курс международного права. В 7 т. Т. 1. Понятие, предмет и система международного права / Ю.А. Баскин [и др.]. М : Юриздат, 1989.

УДК 621.396

Л.В. Борисова, В.А. Светличный

СТРАТЕГИЧЕСКИЕ АСПЕКТЫ БОРЬБЫ С КИБЕРПРЕСТУПЛЕНИЯМИ

Термин «киберпреступность» подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде (Десятый конгресс ООН по предупреждению преступности и обращению с правонарушителями).

Оценить сферу действия, распространенность, стоимость киберпреступлений представляется чрезвычайно сложной задачей. Например, наиболее ловкие и изящно совершенные преступления против (или с использованием) компьютерных систем чаще всего вообще не обнаруживаются даже пострадавшими. Те же, которые выявляются, чаще всего не разглашаются самими пострадавшими, поскольку подобные факты могут повредить их личным или коммерческим интересам.

Мотивы совершения киберпреступлений довольно разнообразны, но часть их можно отнести к «вечным»: жадность, любопытство, месть. Кроме того, в современном обществе месть может иметь еще идеологи-

ческую или религиозную основы. Также значительное место в списке мотивов совершения киберпреступлений занимает едва ли не уникальный в своем роде мотив – интеллектуальная борьба между человеком и компьютерной системой. Изменить или каким-либо образом повлиять на мотивы совершения этих преступлений практически невозможно, поэтому наиболее стратегически выгодным подходом является уменьшение возможностей совершения преступлений и усиление средств контроля и безопасности.

Если мотивы киберпреступлений практически не изменяются, то разнообразие возможностей их совершения постоянно увеличивается. Экспоненциальный рост компьютерных коммуникаций создает параллельные возможности для потенциальных преступников и соответственно создает параллельный риск для потенциальных жертв. Интернет, становясь все больше ареной ведения коммерческой деятельности, соответственно становится и ареной мошеннических операций.

В настоящее время очевиден тот факт, что экономическое благополучие стран зависит от их интеграции. В соответствии с тем, что киберпространство становится основной сферой коммерческих отношений, крайне необходимо обезопасить законную основу ведения коммерческих отношений.

Основой любой юридической защиты от киберпреступлений является законодательно закрепленная база. В связи с глобальной природой самого киберпространства существует необходимость гармонизировать законодательства стран в области киберпреступлений.

Законодательства некоторых стран являются относительно эластичными, т. е. способны «реагировать» на беспрецедентные преступления без необходимости внесения изменений в само законодательство. Законодательства других стран, наоборот, нуждаются во внесении дополнений и поправок для соответствия новым видам преступлений. Например, общепринятое понятие «мошенничества» подразумевает получение какой-либо выгоды обманным путем. Обманом обычно считается воздействие на сознание какого-то человека. Когда же мошенничество направлено против электронной системы, может возникнуть необходимость внесения юридических дополнений для снятия неопределенности. Аналогично и юридические определения воровства или ущерба в некоторых странах могут относиться только к материальным ценностям, т. е. похищение или разрушение собственности в цифровом виде не будет считаться преступлением.

В основном уголовная ответственность должна быть предусмотрена для следующих деяний:

несанкционированный доступ к компьютеру или компьютерной системе;

законное вмешательство для использования компьютера или компьютерной системы;

разрушение или изменение данных в рамках компьютерной системы;

похищение нематериальной собственности;

получение выгоды путем обмана (включительно и электронных систем) [1].

Одним из наиболее важных аспектов киберпреступлений является глобальный доступ, т. е. действия гражданина одной страны могут иметь существенное отражение в разных странах. Отсюда возникают две проблемы в отношении нападений на средства международных телекоммуникаций: во-первых, определение, где именно произошло нападение, чтобы выяснить, какой закон следует применить; во-вторых, получение улик и доказательство того, что преступник может быть выявлен и поставлен перед судом. Обе эти проблемы связаны с множеством сложных юридических вопросов юрисдикции и экстрадиции, например, если on-line реклама, выпущенная в США, содержит неправдивые сведения о компании, находящейся на австралийской бирже, то где же тогда искать виновного: в США, Австралии или где-то еще?

Даже если кому-то удается определить, какой закон в конкретном случае следует применить, может возникнуть множество трудностей с применением этого закона. В унитарной юрисдикции, например, в Новой Зеландии, где действует единое законодательство и единственная правоохранительная организация, определение и применение соответствующего закона является проблемной задачей. Преступления, совершаемые во всем мире, очевидно, ставят еще большие проблемы. Например, телезритель из Украины, столкнувшийся с телевизионным мошенничеством из Польши, не получит особой помощи как со стороны правоохранительных органов Украины, так и Польши. Следовательно, регулирование только по территориальному признаку неприменимо для подобных видов преступлений.

Традиционно юрисдикция судов была региональной. Это значило, что суды могли осуществлять преследование только против лиц, совершивших действия, за которые предусмотрена ответственность на какой-то конкретной территории. Тем не менее существовала возможность консультации региональных судебных органов с экстратерриториальной юрисдикцией по некоторым преступлениям. При некоторых обстоятельствах национальный закон может применяться для преступлений, совершенных за границей иностранными подданными. Но такие случаи крайне редки. Впрочем, в условиях глобализации, когда финансовые трудности, связанные с экстрадицией, практически исчезнут, такие случаи могут стать повседневными.

В дополнение к тому, что международные киберпреступления расследуются в соответствие с международным законодательством, необходимо наличие взаимного международного сотрудничества. Прошлый опыт показывает, что обычно такое сотрудничество происходит без особого энтузиазма, за исключением особых случаев, когда отношение к вопросу вполне однозначно (например, торговля наркотиками или финансовые преступления,

угрожающие привести к потрясениям на мировом рынке) и присутствует единое стремление в решении проблемы. Во многих случаях экстрадиция является тем более проблемной, чем большая культурная и идеологическая разница существует между сторонами.

Для наиболее эффективного действия международного законодательства необходимо существование стабильности в отношениях между независимыми государствами. Такой стабильности пока нет, и вряд ли она в ближайшее время станет возможной. Но, тем не менее, было сделано довольно много на пути международной гармонизации законодательства, касающегося киберпреступлений. В качестве примера можно привести проект соглашения Евросоюза и Совета Европы по киберпреступлениям. Данный проект соглашения содержит общие разделы, относящиеся к уголовному праву, поиску и конфискации электронных данных, юрисдикции, взаимному сотрудничеству [2].

Еще одной серьезной проблемой, по крайней мере, на сегодняшний день, является недостаток высококлассных специалистов в области расследования компьютерных преступлений. Недостаточный уровень заработной платы специалистов в области компьютерных преступлений приводит к «утечки мозгов» из правоохранительных органов в частный бизнес.

Задача тех, кто занимается борьбой с киберпреступлениями, сводится к поиску «золотой середины» между терпимым уровнем незаконности в киберпространстве в обмен на возможность использовать многочисленные преимущества цифровых технологий. На ранней стадии технологической революции в этой области представляется полезным использовать рынок, поскольку рыночные возможности могут предложить более эффективные решения, чем государственное регулирование.

Противодействия компьютерной преступности – комплексная проблема. В настоящее время законы должны соответствовать требованиям, предъявляемым современным уровнем развития технологий. С этой целью необходимо проводить целенаправленную работу по оптимизации законодательства, регулирующих распространение информации в телекоммуникационных сетях. Одним из приоритетных направлений является также организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы и обеспечение их необходимой материально-технической базой.

1. Щетилов А. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом [Электронный ресурс]. Режим доступа: http://www.cnme-research.org.

2. Denning D.E. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. URL: http://www.nautilus.org/info-policy/workshop/papers/denning.html.

УДК 343.98

А.С. Босько

О КИБЕРТЕРРОРИЗМЕ

Термин «кибертерроризм» появился предположительно в 1997 г. Именно тогда специальный агент ФБР Марк Поллитт определил этот вид терроризма как «преднамеренные, политически мотивированные атаки на информационные, компьютерные системы, компьютерные программы и данные, выраженные в применении насилия по отношению к гражданским целям со стороны субнациональных групп или тайных агентов». Известный эксперт Д. Деннинг говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенную с целью принудить органы власти к содействию в достижении политических или социальных целей. Кибертерроризм использует открытость интернета для дискредитации правительств и государств, размещения сайтов террористической направленности, порчи и разрушения ключевых систем путем внесения в них фальсифицированных данных или постоянного вывода этих систем из рабочего состояния, что порождает страх и тревогу и является своего рода дополнением к традиционному виду терроризма.

По нашему мнению, можно выделить два вида кибертерроризма: совершение с помощью компьютеров и компьютерных сетей террористических действий (условно назовем это терроризмом в «чистом виде»), а также использование киберпространства в целях террористических групп, но не для непосредственного совершения терактов.

Первому виду кибертерроризма можно дать определение с помощью соединения понятий «киберпространство» и «терроризм». Терроризм есть совершение взрыва, поджога или иных действий, создающих опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий, если эти действия совершены в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти, а также угроза совершения указанных действий в тех же целях. Таким образом, кибертерроризм «в чистом виде» есть умышленная атака на компьютеры, компьютерные программы, компьютерные сети или обрабатываемую ими информацию, создающая опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий. Такое деяние должно быть совершено в целях нарушения общественной безопасности, устрашения населения либо оказания воздействия на принятие решений органами власти. К такому виду терроризма можно отнести также угрозу совершения подобных действий для достижения вышеуказанных целей.

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования
«Академия Министерства внутренних дел Республики Беларусь»

ТЕОРЕТИЧЕСКИЕ И ПРИКЛАДНЫЕ ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Международная научно-практическая конференция (Минск, 21 июня 2012 г.)

Тезисы докладов

Минск
Академия МВД
2012

УДК 004:34
ББК 32.81
Т33

Редакционная коллегия:
В.Б. Шабанов, А.Н. Лепёхин, Н.М. Бобович, П.Л. Боровик

Т33 **Теоретические и прикладные проблемы информационной безопасности** : тез. докл. Междунар. науч.-практ. конф. (Минск, 21 июня 2012 г.) / М-во внутр. дел Респ. Беларусь, учреждение образования «Акад. М-ва внутр. дел Респ. Беларусь». – Минск : Акад. МВД, 2012. – 331 с.

ISBN 978-985-427-749-3.

Сборник посвящен актуальным проблемам информационной безопасности, анализу перспективных методологических подходов к их решению, вопросам создания и внедрения систем защиты информации в информационные системы правоохранительных органов, а также подготовке специалистов в сфере защиты информации.

УДК 004:34
ББК 32.81

ISBN 978-985-427-749-3

© УО «Академия Министерства внутренних дел Республики Беларусь», 2012