АКТУАЛЬНЫЕ ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И БОРЬБЫ С КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТЬЮ

УДК 004.3:34

И.С. Андреев, А.Г. Вильмак, Т.Г. Чудиловская

О ПРАВОВОМ РЕГУЛИРОВАНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Развитие информационной сферы, обеспечение ее безопасности становятся одними из приоритетных задач национальной политики развитых стран мира. Согласно Стратегии развития информационного общества в Республике Беларусь, утвержденной постановлением Совета Министров Республики Беларусь от 9 августа 2010 г. № 1174, вопросы обеспечения национальной безопасности в информационной сфере отнесены к числу главных задач, направленных на развитие информационного общества в Республике Беларусь.

Задача укрепления безопасности государства в информационной сфере определена Концепцией национальной безопасности, утвержденной указом Президента Республики Беларусь от 9 ноября 2010 г. № 575 (далее – Концепция), в числе важных задач обеспечения национальной безопасности.

В соответствии с п. 4 Концепции информационная безопасность – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере. Для достижения такого баланса необходимо наличие определенных правил поведения или социальных норм, среди которых особое значение придается правовым требованиям, устанавливаемым в официальных документах уполномоченными государственными органами.

Правовое обеспечение информационной безопасности представляет собой деятельность законодательных и исполнительных органов государственной власти по разработке, реализации и контролю исполнения совокупности нормативных правовых актов, регламентирующих практическую деятельность по защите информации личности, общества и государства.

Правовое обеспечение информационной безопасности направлено:

на обеспечение эффективной реализации и защиту конституционных прав личности;

неприкосновенность частной жизни, личную и семейную тайну, защиту чести и достоинства;

создание благоприятных условий для свободного и оперативного доступа к информации органов государственной власти и органов местного самоуправления, непосредственно затрагивающей права и свободы личности;

защиту прав участников электронной коммерции;

защиту интеллектуальной собственности;

обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, и иной информации с ограниченным доступом;

защиту интересов государства и общества в сфере использования государственных информационных ресурсов и т. д.

Правовое обеспечение призвано создать и поддерживать в обществе негативное отношение к нарушителям информационной безопасности и, в частности, сформировать карательные меры воздействия к злостным нарушителям. В состав этой части обеспечения безопасности входят:

Конституция Республики Беларусь;

законы Республики Беларусь, касающиеся информатизации и информационной безопасности;

подзаконные акты (указы Президента Республики Беларусь, кодексы, постановления Совета Министров Республики Беларусь, стандарты и другие нормативные документы);

международные договоры, в том числе об оказании взаимной правовой помощи, ратифицированные в Республике Беларусь.

Среди основных нормативных правовых актов в области информационной безопасности особое место принадлежит законам Республики Беларусь «Об информации, информатизации и защите информации» от 10 ноября 2008 г. № 455-З и «Об электронном документе и электронной цифровой подписи» от 28 декабря 2009 г. № 113-З.

К подзаконным нормативным правовым актам, регулирующим отношения по вопросам доступа граждан к информации, защите информации, компетенции органов государственного управления в сфере защиты информации, определении компетенции органов государственного управления в сфере защиты информации, международному сотрудничеству можно отнести указ Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети интернет», постановление Совета Министров Республики Беларусь от 29 апреля 2010 г. № 645 «О некоторых вопросах интернет-сайтов государственных органов и организаций и признании утратившим силу постановления Совета Министров Республики Беларусь от 11 февраля 2006 г. № 192», постановление Совета Министров Республики Беларусь от 26 мая 2009 г. № 675 «О некоторых вопросах защиты информации» и т. д.

Анализируя проблемы систематизации законодательства в сфере обеспечения информационной безопасности, ученые делают вывод, что система законодательства в данной области включает нормы конституционного, административного, гражданского, уголовного, трудового и ряда других отраслей права.

Вся деятельность по правовому обеспечению информационной безопасности должна строиться на основе трех фундаментальных положений

права: соблюдении законности, обеспечении баланса интересов отдельных субъектов и государства, неотвратимости наказания.

Для обеспечения информационной безопасности необходимо наличие соответствующих органов, организаций, ведомств и обеспечение их эффективного функционирования. В Республике Беларусь ключевыми являются Оперативно-аналитический центр при Президенте Республики Беларусь, управление «К», Комитет государственной безопасности. Данные органы, благодаря своей четкой структуре и профессиональному опыту, обеспечивают определенный уровень информационной безопасности в республике.

Разработка и совершенствование законодательной базы информационной безопасности, направленной на восполнение пробелов в правовом регулировании общественных отношений в информационной сфере, является необходимой мерой для формирования информационного общества в Республике Беларусь.

УДК 621.396

Л.В. Борисова, Ю.Н. Онищенко

КИБЕРПРЕСТУПНОСТЬ: МЕЖДУНАРОДНО-ПРАВОВОЙ АСПЕКТ

Интернет «ликвидирует» границы и «территориальность». Пока существуют огромные объемы данных, связанных с помощью интернета, эта сеть, без сомнения, является единственной (и наиболее важной) информационной сетью в мире, что также дает возможность людям, сидящим перед компьютером в одной стране, иметь неограниченные возможности по воздействию на компьютеры, находящиеся в других странах.

Преступники очень быстро осознали масштабы возможностей, предоставляемых интернетом и электронными коммуникациями.

Среди всех киберпреступлений, совершаемых в мире, все больше становится так называемых «международных», т. е. использующих в качестве средств (жертв) информационные системы, расположенные в различных странах. В таких случаях требуется проведение большого, комплексного и тщательного расследования. Преступный потенциал киберпреступлений, включающий шпионаж и саботаж, представляет большое беспокойство для всех стран. Но следует учесть, что даже простое и бесхитростное использование интернета может применяться для совершения вполне «традиционных» преступлений. Примером является продажа информации о кредитных картах, мошенничество при продаже товаров через интернет с последующим непредоставлением оных, невыполнение других торговых обязательств и т. д.

Различные организации опубликовали списки наиболее распространенных, по их мнению, форм мошеннической деятельности в интернете.

Такая деятельность хотя и более безвредна, по сравнению с другими формами преступной деятельности, но потенциально может повредить доверию к интернету как к среде ведения электронной коммерции.

Киберпреступники могут применять так называемые «разветвленные» атаки на сайты, например, государственных органов власти и т. д. При проведении данных атак используется большое число компьютеров, которые могут быть как «сознательными» участниками, так и невольными «сообщниками», будучи пораженными различными типами вирусов. Поскольку в нападении может принимать участие множество компьютеров, и они могут быть запрограммированы уничтожить «вирусный» код после проведения атаки, такие атаки чрезвычайно сложно отследить.

Следующим важным аспектом является развитие технологий шифрования. При их использовании преступники смогут хранить информацию, которая, будучи обнаруженной, вряд ли с легкостью может быть дешифрована.

Осуществление расследования киберпреступлений довольно сложно в любой стране мира. Практически невозможно гарантировать, что свидетельства (улики) могут быть получены, изолированы от вмешательства и вообще допустимы для представления в суде. Когда к таким проблемам добавляется элемент «интернациональности», то полученная смесь становится еще более «горькой».

Для эффективного взаимодействия правоохранительных ведомств разных государств в сфере борьбы с киберпреступностью необходимо открыть канал связи с соответствующими полномочиями, что обеспечит обслуживание оперативных запросов в любое время дня и ночи во всех часовых поясах. Также международному сотрудничеству в немалой степени могут мешать различные юридические разногласия.

До тех пор пока большинство стран мира не примет законы, предусматривающие уголовную ответственность за преступления, совершенные в киберпространстве, юридические «дыры» будут делать международное сотрудничество в данной области невозможным. В настоящее время большая часть мирового сообщества все еще не достаточно готова к борьбе с киберпреступлениями.

Более того, даже если каждая страна примет требуемую законодательную базу, при расследовании киберпреступлений будет необходима помощь специальных представителей для исследования особенностей законодательств этих стран. Еще следует отметить, что область киберпреступлений принадлежит к области так называемых «высоких» технологий и необходимо, чтобы все страны обладали достаточно высоким техническим потенциалом в данной области. Следовательно, мировое сообщество должно сосредоточить свои усилия на помощи менее развитым государствам. Важно понимать, что проблема киберпреступлений – проблема не только «богатых» стран, только общими усилиями и сотрудничеством можно ее решить. Существуют несколько путей эффективной борьбы с киберпреступлениями: односторонние действия, частичное или всестороннее сотрудничество.