СОВЕРШЕНСТВОВАНИЕ МЕХАНИЗМОВ ПРОТИВОДЕЙСТВИЯ КОМПЬЮТЕРНОЙ ПРЕСТУПНОСТИ: МЕЖДУНАРОДНЫЙ И НАЦИОНАЛЬНЫЙ ОПЫТ

В. О. Сень

Гомельский государственный технический университет имени П. О. Сухого, Беларусь

Научный руководитель канд. юрид. наук, доц. С. П. Кацубо

Обеспокоенность мирового сообщества ростом количества компьютерных правонарушений определяет многочисленные попытки создания национальных и международных механизмов (прежде всего – правовых) противодействия подобным общественно опасным проявлениям. Именно этим обстоятельством объясняется постоянная работа над созданием, совершенствованием и реализацией международных нормативных правовых документов, посвященных повышению эффективности взаимодействия правоохранительных органов в условиях глобальной информатизации.

Важное значение при этом отводится международному сотрудничеству. Так, в Директиве Европейского парламента и Совета от 22 мая 2001 г. № 2001/29/ЕС специальная глава посвящена вопросам применения технических средств защиты и использования информации об управлении правами. Весьма значительным событием стало также подписание лидерами стран «восьмерки» Окинавской Хартии глобального информационного общества. Данный документ можно позиционировать в качестве рекомендаций по объединению мирового информационного сообщества и формированию единых представлений и правил по созданию и совершенствованию правовых механизмов по регулированию возникающих общественных отношений. Окинавская Хартия обозначила необходимость поиска компромиссного решения между доступностью информационных ресурсов глобальных сетей, соблюдением прав и свобод человека в информационной сфере и регулированием общественных отношений при создании, распоряжении и использовании таких ресурсов путем наложения определенных ограничений и обязанностей на субъекты, создающие, использующие, распространяющие и предоставляющие их. Отмечается, что усилия международного сообщества, направленные на развитие глобального информационного общества, должны сопровождаться согласованными действиями по созданию безопасного и свободного от преступности киберпространства.

Страны Европейского Союза последовательно проводят политику сотрудничества в области противодействия компьютерной преступности. Так, с целью унификации национальных законодательств в 1989 г. Комитетом министров Европейского Совета был согласован и утвержден Список правонарушений, рекомендованный странам-участницам ЕС для разработки единой уголовной стратегии, связанной с компьютерными преступлениями, содержащий восемь видов компьютерных преступлений. 23 ноября 2001 г. в Будапеште была подписана Международная конвенция о киберпреступности.

Международное сотрудничество в противодействии компьютерной преступности значительно затруднено, если в законодательствах разных стран существуют различные подходы к установлению ответственности за совершение одних и тех же общественно опасных деяний. Для повышения эффективности взаимодействия правоохранительных органов разных стран предпринимается попытка гармонизации национальных законодательств путем выдачи рекомендаций по выработке схожих процессов сбора доказательств о совершении компьютерных преступлений в электронной форме.

В силу отсутствия безупречного правового механизма защиты прав в Интернете в настоящее время используются и технические методы защиты своих произведений. Существует множество систем и технических средств защиты объектов авторского права в цифровой форме, позволяющих более или менее удачно защищать в сети права авторов и иных правообладателей: идентификаторы, цифровые марки, цифровые водяные знаки; цифровые подписи, а также использование аппаратных ключей, привязка к индивидуальным особенностям аппаратуры; ограничение доступа к объектам авторского права, содержащимся в Интернете; методы криптографического преобразования материала (шифрование). Однако, находятся все более совершенные технологии, позволяющие разрушить любую защиту. Поэтому весьма важно не только формально закрепить за авторами право на техническую защиту своих интересов, но и интенсивно развивать соответствующие меры противодействия преступным посягательствам. Необходимость формирования современных механизмов за-

щиты объектов авторского права приводит к поиску оптимального, взаимодополняющего сочетания правовых и технологических мер защиты.

Правовую основу для формирования и проведения единой государственной политики в области информатизации и защиты информации составляет совокупность нормативных правовых актов, устанавливающих приоритет национальных интересов при решении вопросов безопасности информации, в том числе частной информации. Сегодня в мире более двадцати стран имеют национальное законодательство, относящееся к использованию глобального информационного пространства.

Так, Канадская ассоциация провайдеров услуг Интернет разработала модельный кодекс по защите персональной информации, помочь членам ассоциации в своей деятельности соответствовать правовым стандартам, не распространять информацию незаконного содержания, реагировать на информацию пользователей о наличии такого содержания в Интернет. Во Франции создан официальный сайт Хартии Интернет, в котором определены принципы добровольных обязательств пользователей и создателей информационных услуг и продуктов, связанных с Интернет. В Швейцарии разработаны рекомендации для провайдеров Интернет. Так, провайдеры должны знать, что наказание за демонстрацию сцен насилия в соответствии с Уголовным кодексом Швейцарии не ограничивается кино- или фотопрезентациями, но распространяется и на другие формы презентаций, в том числе на компьютерные игры. Это же положение относится к порнографии. Провайдеры должны информировать потребителей о потенциальных проблемах, связанных с защитой данных, используемых в Интернет. Особое внимание они должны уделять мерам по сохранению конфиденциальности и точности персональных данных, ограничению доступа к ним.

В шведском законе, регулирующем ответственность владельцев досок объявлений, устанавливается, что таковые обязаны удалять сообщения третьих лиц в том случае, если содержащаяся в них информация нарушает ряд норм уголовного и гражданского законодательства (в части авторского права). Схожая с европейской, но менее детальная схема ответственности при нарушении авторских прав, определена в США. В Англии также действует законодательный акт, который регулирует ответственность Интернет-провайдеров за достоверность размещаемой на их сайтах информации.

В Российской Федерации разработаны рекомендации по организации деятельности лиц в сфере интернет-коммерции, согласно которым провайдер не несет ответственности за незаконные действия лиц, использующих его услуги, в случае отсутствия информации об указанных действиях или возможности своевременно и достоверно выявить и/или квалифицировать указанные действия. Он также не несет ответственности за действия лиц, использующих его услуги и нарушивших обычаи делового оборота в сфере использования сети Интернет, если иное не предусмотрено законом или договором.

В Республике Беларусь Постановлением Совета Министров Республики Беларусь от 09.08.2010 г. № 1174 утверждена Стратегия развития информационного общества в Республике Беларусь на период до 2015 г., которая определяет цель, задачи, условия и приоритетные направления развития информационного общества в Республике Беларусь, механизм и ожидаемые результаты от ее реализации.

Приоритетными направлениями деятельности в области обеспечения информационной безопасности являются: развитие правового обеспечения информационной безопасности и совершенствование правоохранительной деятельности в этой сфере;

разработка и внедрение эффективных программных и программно-аппаратных средств защиты информационных ресурсов, информационных и телекоммуникационных систем; совершенствование системы повышения квалификации и создание системы переподготовки кадров в этой области; формирование системы мониторинга информационной безопасности Республики Беларусь в наиболее важных сферах жизнедеятельности общества и государства.

В условиях стремительно развивающегося рынка электронных услуг и электронной торговли актуальными являются вопросы цифрового доверия. Первоочередными задачами являются: создание государственной системы управления открытыми ключами; широкомасштабное внедрение средств электронной цифровой подписи; разработка типовых политик безопасности для государственных информационных систем; создание системы идентификации для физических и юридических лиц, что позволит свести к минимуму возможность злоупотребления персональной и иной конфиденциальной информацией. Для юридических и физических лиц должны быть созданы доступные в ценовом и техническом аспекте механизмы и средства, обеспечивающие идентификацию и аутентификацию пользователей, конфиденциальность и целостность сообщений в системах и сетях общего пользования. Это позволит расширить сферу использования электронного документооборота, обеспечит возможность ведения электронной торговли, предоставления электронных услуг, широкомасштабного внедрения систем электронных платежей.

Положением о порядке ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению в соответствии с законодательными актами, утвержденным Постановлением Оперативно-аналитического центра при Президенте Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 29.06.2010 г. № 4/11, устанавливается порядок ограничения доступа пользователей интернет-услуг к информации, запрещенной к распространению, содержание которой направлено на: осуществление экстремистской деятельности; незаконный оборот оружия, боеприпасов, взрывных устройств, взрывчатых, радиоактивных, отравляющих, сильнодействующих, ядовитых, токсических веществ, наркотических средств, психотропных веществ; содействие незаконной миграции и торговле людьми; распространение порнографических материалов; пропаганду насилия, жестокости и других деяний, запрещенных законодательством.

Поставщики интернет-услуг, непосредственно оказывающие услуги по ограничению доступа, обязаны: ввести в эксплуатацию систему ограничения доступа и обеспечить ее качественное функционирование; определить лиц, ответственных за функционирование системы ограничения доступа; обеспечить возможность настройки системы ограничения доступа только из внутреннего сегмента сети поставщика интернет-услуг; незамедлительно устранять нарушения, связанные с оказанием услуг по ограничению доступа.

Таким образом, отмечается активизация деятельности в области пресечения преступных посягательств на информационные ресурсы как на международном уровне, так и в Республике Беларусь. Осуществляется взаимодействие на межгосударственном уровне в области развития и обеспечения безопасности использования информационных технологий, разрабатывается механизм противодействия компьютерной преступности.