УДК 004:34

А.В. Фурманов, Т.Г. Чудиловская

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ – УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ

Современные информационные технологии не только открывают безграничные возможности, но и порождают новые проблемы развития общества, несут новые опасности, вызовы и угрозы его безопасности, одной из важнейших составляющих которой является информационная безопасность. Практически все страны с развитой экономикой на уровне государственных органов, предпринимательских структур разрабатывают и применяют комплексные меры, направленные на обеспечение информационной безопасности.

В силу трансграничности угроз информационной безопасности эффективное противодействие правонарушениям, совершаемым с использованием информационных технологий, может быть обеспечено на основе тесного взаимодействия государств – участников Содружества Независимых Государств между собой и с другими государствами.

Одним из основных направлений сотрудничества государств – участников СНГ является выработка рекомендаций и предложений по совершенствованию правового обеспечения информационной безопасности.

В феврале 1996 г. был принят модельный Уголовный кодекс для государств – участников СНГ (далее – модельный УК), который содержит отдельную главу 30 «Преступления против информационной безопасности», состоящую из семи статей (ст. 286–292). Принятие данного документа обратило внимание государств – участников СНГ на необходимость уголовно-правовой защиты отношений, складывающихся в сфере обеспечения информационной безопасности.

На сегодняшний день все государства СНГ включили в принятые после обретения независимости уголовные кодексы самостоятельные главы, предусматривающие уголовную ответственность за компьютерные преступления. Однако необходимо заметить, что в уголовных законах государств – участников СНГ отсутствует единство подходов к определению терминов, что не способствует унификации уголовного законодательства стран СНГ в рассматриваемой области.

Для укрепления правовой основы борьбы с преступностью в информационной сфере 1 июня 2001 г. было подписано Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, которое является правовой

основой сотрудничества правоохранительных и судебных органов государств – участников СНГ в области обеспечения эффективного предупреждения, выявления, пресечения, раскрытия и расследования компьютерных преступлений.

Важным нормативным актом по сближению национальных законодательств, регулирующим информационные отношения, является модельный Закон «Об информатизации, информации и защите информации», принятый 18 ноября 2005 г. на 26-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ.

В рамках СНГ также принята Концепция сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности, утвержденная Решением Совета глав государств Содружества Независимых Государств 10 октября 2008 г. В документе определены основные цели и принципы сотрудничества в сфере обеспечения информационной безопасности, угрозы информационной безопасности, методы и основные направления сотрудничества, план мероприятий. Концепция явилась основанием для Рекомендаций по совершенствованию и гармонизации национального законодательства государств – участников СНГ в сфере обеспечения информационной безопасности, которые приняты на 38-м пленарном заседании Межпарламентской Ассамблеи государств – участников СНГ.

В настоящее время преступления, совершаемые с использованием информационных технологий, приобретают транснациональный и организованный характер, создают угрозу национальной безопасности государств – участников СНГ; происходит сращивание различных видов преступности, главным образом за счет использования средств компьютерной техники и информационных сетей. В связи с этим была принята Концепция сотрудничества государств – участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, одобренная Решением Совета глав государств СНГ 25 октября 2013 г. Концепция определяет принципы, задачи, основные направления, формы и систему обеспечения сотрудничества.

Для осуществления взаимодействия при выполнении положений Концепции сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности с учетом важности совместного и эффективного использования новейших информационно-коммуникационных технологий для усиления противодействия угрозам информационной безопасности 20 ноября 2013 г. заключено Соглашение о сотрудничестве государств – участников СНГ в области обеспечения информационной безопасности. Целью документа является проведение совместных скоординированных мероприятий, направленных на обеспечение информационной безопасности.

Для обеспечения решения задач устойчивого развития информационных отношений, надежной защиты от реализации угроз жизненно важным интересам личности, общества и государства в информационной сфере 28 октября 2016 г. Советом глав правительств СНГ утверждена Стратегия сотрудничества государств – участников СНГ в построении и развитии информационного общества на период до 2025 года и План действий по ее реализации.

В документе определены основные направления взаимодействия государств – участников СНГ в области информационной безопасности:

разработка и обоснование предложений по структуре и задачам коллективной системы информационной безопасности государств – участников СНГ;

поощрение дальнейшего укрепления доверия и основ безопасности посредством дополняющих и взаимоукрепляющих инициатив в области безопасности при использовании информационно-компьютерных технологий;

защита национальных и межгосударственных информационных систем от несанкционированного доступа, от утечки защищаемой информации по техническим каналам и от внешнего электромагнитного воздействия;

защита баз данных и информационных ресурсов;

защита персональных данных и прав субъектов информации;

обеспечение безопасности информационных и коммуникационных технологий, сетей и систем;

создание защищенных систем межведомственного электронного документооборота;

развитие механизмов мониторинга и противодействия киберпреступности;

обеспечение взаимодействия национальных центров реагирования на компьютерные инциденты;

выявление и оперативное реагирование на случаи нарушения информационной безопасности, обмен информацией и техническими средствами борьбы с нарушениями;

формирование систем мониторинга ресурсов национальных сегментов интернета в целях своевременного выявления угроз, а также поиска оптимальных средств их нейтрализации;

создание инфраструктуры, необходимой для внедрения электронной цифровой подписи;

подготовка и реализация совместных мероприятий и проектов по формированию культуры обеспечения информационной безопасности.

Краткий обзор документов в сфере обеспечения информационной безопасности показывает, что нормотворческий процесс на пространстве СНГ протекает довольно динамично. Информационная политика государств – участников СНГ направлена на установление общих подходов к правовому регулированию обеспечения информационной безопасности, укреплению сбалансированности национальных правовых систем в условиях информатизации общества; на развитие международного информационного обмена; на обеспечение безопасности информационных условий экономического и таможенного сотрудничества; на стимулирование использования информационно-коммуникативных технологий во всех сферах жизни общества.

Однако принимаемые в рамках СНГ документы не в полной мере согласованы между собой. Для решения задач правового регулирования отношений в сфере обеспечения информационной безопасности исключительно важным является вопрос проработки правовых дефиниций с целью однозначного их толкования. Унификация основных терминов и понятий в нормативной правовой базе государств – участников СНГ – важное направление совершенствования законодательства.

Актуальным является и решение вопроса о юридической силе правовых актов СНГ для Республики Беларусь и иных государств – участников СНГ, так как на уровне учредительных документов отсутствует четкая система международно-правовых актов, принимаемых органами СНГ, – их виды, соотношения между собой по юридической силе и степени обязательности.

УДК 341.24:342.97

С.А. Чернышева

МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В БОРЬБЕ С КОМПЬЮТЕРНОЙ ПРЕСТУПЛЕНОСТЬЮ

Компьютерная преступность (киберпреступность или кибертерроризм), являясь принципиально новым видом нарушений в информационной сфере, характеризуется способностью быстро приспосабливаться к новым условиям и проникать во все сферы жизни общества.

Компьютерная преступность превратилась в целую криминальную отрасль. Возможности быстро развивающихся информационно-компьютерных технологий (ИКТ) все активнее используются в преступных целях, о чем свидетельствует статистика компьютерных преступлений как в Республике Беларусь, так и в зарубежных странах.

Так, в Республике Беларусь в 2016 г. число выявленных преступлений в сфере высоких технологий увеличилось на 1,3 % в сравнении с 2015 г., а общий уровень раскрываемости составил 56,5 % (в 2015 г. – 55,5 %).