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 %).

Увеличение количества компьютерных преступлений произошло за счет прироста преступлений против информационной безопасности на 63,6 % (с 404 до 651). Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (с 102 до 258).

Столкнувшись с компьютерной преступностью, органы уголовной юстиции зарубежных стран начали борьбу с ней путем применения к злоумышленникам традиционных норм о хищениях или злоупотреблениях. Однако такой подход оказался неудачным. Компьютерные преступления не укладывались в диспозиции норм об ответственности за названные преступления. В них не был учтен способ совершения преступлений (использование высоких технологий), личность преступника и общественно опасные последствия, которые исчислялись миллиардами долларов США.

Стали возникать новые нормы уголовного права, предусматривающие ответственность за новый вид преступности – компьютерные преступления.

Впервые закон о компьютерных преступлениях был принят 2 апреля 1973 г. в Швеции. В начале 1990-х гг. Уголовный кодекс Швеции был дополнен нормами, предусматривающими ответственность за деяния с использованием компьютерной информации и технологий.

В 1979 г. на конференции Американской ассоциации адвокатов впервые в США была сформирована система компьютерных преступлений, ставшая затем основой для уголовного законодательства штатов.

Вопросами борьбы с компьютерными преступлениями стали заниматься и международные организации.

С 1983 по 1985 г. Комитет Организации экономического сотрудничества и развития (ОЭСР) обсудил возможность международной гармонизации уголовного законодательства отдельных государств в целях борьбы с экономическими компьютерными преступлениями. В 1986 г. Комитетом был предложен единый перечень действий, которые должны рассматриваться в законодательстве государств – членов организации как компьютерные преступления.

В период с 1985 по 1989 г. над проблемой компьютерных преступлений работал Отдельный комитет экспертов по компьютерным преступлениям Совета Европы.

Развитие законодательства об ответственности за компьютерные преступления в ряде стран Европы происходило следующим образом. В 1986 г. Уголовный кодекс ФРГ был дополнен нормами, предусматривающими ответственность за компьютерные преступления. В августе 1990 г. вступил в силу Закон о злоупотреблениях компьютерами в

Великобритании. В 1993 г. Уголовный кодекс Нидерландов был дополнен новыми составами преступлений и т. д.

Особого внимания заслуживает опыт борьбы с компьютерной преступностью в Японии, которая в дополнение к нормам Уголовного кодекса о компьютерных преступлениях приняла 3 февраля 2000 г. Закон «О несанкционированном проникновении в компьютерные сети».

В первой половине 1990-х гг. законы об ответственности за компьютерные преступления были приняты и в других государствах мира.

Однако борьба с транснациональной организованной компьютерной преступностью требовала выработки более эффективных мер. Различия в правовых системах при недостаточно развитом международном сотрудничестве усложняли проведение расследований киберпреступлений и преследование за их совершение.

Эксперты ООН на XI Конгрессе (Бангкок, 2005) подчеркивали особый характер компьютерной преступности и указывали на необходимость применения комплексных подходов в борьбе с ней, а также на неотложность обновления уголовного законодательства всех развитых стран, в том числе введение норм, касающихся новых видов компьютерной преступности.

В настоящее время разработаны и действуют следующие международно-правовые основы сотрудничества в области борьбы с компьютерной преступностью:

Конвенция Совета Европы о киберпреступности 2001 г.;

Меры по борьбе против преступлений, связанных с использованием компьютеров, принятые на XI Конгрессе Организации Объединенных Наций по предупреждению преступности и обращению с правонарушителями в Бангкоке 25 апреля 2005 г.;

Глобальная программа кибербезопасности, утвержденная Международным союзом электросвязи в 2007 г.;

Окинавская Хартия глобального информационного общества, принятая 23 июля 2000 г. на Окинаве (Япония);

Соглашение о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации, заключенное 1 июня 2001 г. и др.

Главным органом в области межгосударственной борьбы с преступностью является Организация Объединенных Наций, которая с 1950 г. на Конгрессах ООН уделяет серьезное внимание проблеме борьбы с компьютерными преступлениями, и эта деятельность включена в число приоритетов ООН.

В частности, на XII Конгрессе ООН (Бразилия, апрель 2010 г.) была рассмотрена рекомендация относительно необходимости тщательного

изучения и принятия решения по разработке глобальной Конвенции о борьбе с киберпреступностью.

Республика Беларусь принимает активное участие в деле международной борьбы с компьютерной преступностью. Наряду с Уголовным кодексом Республики Беларусь (гл. 31) приняты значимые нормативные документы. Правовая база Республики Беларусь в отношении правонарушений и преступлений в информационном пространстве значительно приближена к требованиям и стандартам, принятым на международном уровне, в том числе Конвенции Совета Европы о киберпреступности 2001 г.

В Республике Беларусь Министерство юстиции, Управление «К» Министерства внутренних дел, Комитет государственной безопасности в целях противодействия киберпреступности осуществляют оперативный обмен информацией через международную сеть национальных контактных пунктов (НКП).

Указанная сеть НКП имеется в 58 странах мира (Россия, Украина, США, Германия, Великобритания, Испания, Швеция, Бразилия и др.). Вступление Беларуси в конце 2008 г. в международную сеть НКП способствовало как повышению эффективности работы по противодействию киберпреступности, так и дальнейшему развитию международного сотрудничества МВД Республики Беларусь в целом.

Во многих странах все еще практически отсутствует законодательное обеспечение борьбы с преступностью в киберпространстве, или страны имеют во многом устаревшие законы и механизмы их реализации. При этом понимание масштабов компьютерной преступности приводит к выводу, что справиться с угрозами возможно только совместными усилиями.

Построение деятельности правоохранительных структур на основе внедрения информационных технологий дает совершенно новые возможности для координации совместной деятельности в международном масштабе. Только совместная деятельность и межгосударственное сотрудничество способны эффективно противостоять преступности.

В настоящее время наблюдается осознанная тенденция к унификации законодательства и координации правоохранительной деятельности в мировом масштабе. Вопросы юрисдикции должны решается путем сотрудничества государств.

Универсальным регулятором в сфере борьбы с компьютерной преступностью могла бы стать отдельная Конвенция ООН о компьютерных преступлениях. Значение принятия такой Конвенции необычайно велико.

УДК 343

С.А. Шарапов

О ТЕНДЕНЦИЯХ КРИМИНАЛИЗАЦИИ ДЕЙСТВИЙ С ВРЕДОНОСНЫМИ ПРОГРАММАМИ

В современных условиях практически каждый пользователь компьютера сталкивался с действием вредоносных программ. По данным «Лаборатории Касперского» в 2016 г. при серфинге в интернете атакам вредоносных объектов подверглись 31,9 % компьютеров пользователей. Разработанными указанной компанией программными средствами отражено свыше 758 млн атак, веб-антивирусом обнаружено более 69,2 млн уникальных детектируемых объектов.

Приведенные сведения указывают на значительную актуальность вопроса ответственности за использование вредоносного программного обеспечения и важности его разрешения для общества и государства. Между тем четкие критерии, по которым программы должны относится к категории вредоносных, на законодательном уровне не определены, что влечет за собой формирование противоречивой правоприменительной практики.

В настоящее время в научной литературе активно высказываются предложения о необходимости повышения криминализации как самого понятия «вредоносные программы», так и действий с ними. Например, К.Н. Евдокимов в опубликованной в 2013 г. монографии «Создание, использование и распространение вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты», рекомендованной для использования преподавателями, аспирантами, студентами, слушателями юридических вузов, сотрудниками правоохранительных органов, утверждает, что вредоносную компьютерную программу необходимо рассматривать в широком смысле «как любую компьютерную программу, приводящую к уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации без согласия и уведомления ее владельца (пользователя). Тем самым вредоносными программами могут быть и обычные лицензионные компьютерные программы в случае их использования при совершении преступного деяния и достижения вредных последствий, указанных в статье 273 УК Российской Федерации».

Кроме того, К.Н. Евдокимов предлагает «в число преступных действий включить такое деяние, как приобретение компьютерных программ либо иной компьютерной информации, заведомо предназначен-