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-

ных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации» (аналогичное предложение в 2008 г. высказывалось Е.А. Маслаковой в диссертации на соискание ученой степени кандидата юридических наук «Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты»).

В 2016 г. Д.И. Макушев в статье «О совершенствовании объективной стороны состава преступления, предусмотренного ст. 273 УК Российской Федерации», поддерживая мнение своего научного руководителя – вышеупомянутого К.Н. Евдокимова, утверждает, что «даже поверхностный взгляд на диспозицию ст. 273 УК РФ позволяет сделать вывод об отсутствии наказания за приобретение преступниками вредоносного программного обеспечения». В этой связи он предлагает ввести уголовную ответственность за приобретение вредоносных программ вне зависимости от преступных целей и мотивов. По мнению данного автора, вредоносные компьютерные программы так же, как и оружие, наркотики, взрывчатые вещества, должны считаться предметами, запрещенными к свободному гражданскому обороту, поскольку наносят ущерб информационной безопасности и могут использоваться как орудие либо средство для совершения других компьютерных преступлений. При этом, описывая вредоносные программы, автор относит к их числу компьютерные вирусы (черви, троянские кони, логические бомбы и др.), что не вполне объективно, поскольку они не имеют механизма самовоспроизведения путем внедрения своего кода в другую программу. Указанный в статье результат действия вредоносной программы – «уход от уплаты налогов» также представляется невозможным, хотя схожий тезис приводится, например, в комментарии к Уголовному кодексу Российской Федерации под редакцией А.В. Бриллиантова. Безусловно, при уклонении от уплаты налогов в современных условиях используются средства компьютерной техники и соответствующее программное обеспечение, но можно ли его рассматривать в качестве вредоносного?

В ходе расследования уголовных дел в сфере экономики и в финансово-кредитной системе автор сталкивался со случаями, когда в целях уклонения от уплаты налогов производились определенные манипуляции в программе «1С: Бухгалтерия» (таким образом значительная часть доходов коммерческой структуры была сокрыта от налогообложения), а для хищения денежных средств бухгалтером предприятия вносились изменения в программу для начисления заработной платы работникам.

Такие действия виновных были квалифицированы по соответствующим статьям Уголовного кодекса Республики Беларусь: за уклонение от уплаты налогов было предъявлено обвинение по ст. 243, а за хищение – по ст. 211 УК Республики Беларусь). При этом дополнительная квалификация таких действий по статье за использование вредоносных программ не требуется, несмотря на то, что они действительно совершены с использованием компьютерной техники, соответствующего программного обеспечения и ими причинен вред.

Вышеописанные юридические толкования понятия «вредоносные программы» и предложения по введению уголовной ответственности за их приобретение представляются не вполне оправданными, поскольку приведут к излишней криминализации действий в информационной сфере.

По нашему мнению, вредоносная программа должна предназначаться только для противоправных действий. В этой связи предложение о возможности оценки какой-либо легальной, лицензионной программы как вредоносной, полагаем, является неверным, ибо так можно, например, оценить операционную систему, поскольку она всегда используется при совершении преступлений против информационной безопасности или хищений с использованием компьютерной техники.

Таким образом, необходимо различать (по крайней мере, с точки зрения уголовного права) компьютерные программы, которые могут использоваться для совершения противоправных деяний: они могут быть как легальными и лицензионными, так и сами по себе вредоносными, являющимися таковыми изначально.

В части предложения о введении уголовной ответственности за приобретение вредоносных программ, полагаем, что такая мера будет излишней и чрезмерной, поскольку такое деяние не обладает уровнем общественной опасности, присущей преступлению. А кроме того, действующий уголовный закон позволяет привлечь виновных к ответственности за приобретение таких программ, как за приготовление к преступлению, если установлен умысел в использовании их в противоправных целях.

С учетом изложенного представляется, что любые предложения по ужесточению уголовной ответственности как за преступления против информационной безопасности, так и за иные категории преступлений должны быть качественно и всесторонне проработаны, научно обоснованы не только с точки зрения необходимости и целесообразности, но и с точки зрения последствий их введения.