НЕОБХОДИМОСТЬ ОБЩИХ ПОДХОДОВ В ПРИМЕНЕНИИ МЕР УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В РЕСПУБЛИКЕ БЕЛАРУСЬ, РОССИЙСКОЙ ФЕДЕРАЦИИ И УКРАИНЕ

Н.А. Костюченко

Учреждение образования «Гомельский государственный технический университет имени П.О. Сухого», Республика Беларусь

Развитие современного общества немыслимо без широкого внедрения во все сферы электронно-вычислительной техники. Особую тревогу в этом плане вызывает факт появления и развития в странах СНГ нового вида преступных посягательств, ранее неизвестных юридической науке и практике, и связанный с использованием средств компьютерной техники и информационных технологий, – компьютерных преступлений. Последние потребовали от законодателя принятия срочных правовых мер противодействия этому виду преступности. В частности, законодатели Беларуси, России и Украины ввели в уголовные кодексы стран главы, посвященные этим видам преступлений. Однако, несмотря на схожесть правовых систем, следует указать на различия в закреплении ответственности за преступные деяния в сфере компьютерных технологий. Называя в обиходе эту группу преступлений «компьютерными», законодатель Беларуси употребляет в Уголовном кодексе название «преступления против информационной безопасности», законодатель России – «преступления в сфере компьютерной информации», законодатель Украины – «преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей». Названия соответствующих глав кодекса указывают на родовой объект, который, по сути, также различен.

Исходя из названия главы 31 УК Беларуси, просматривается родовой объект – информационная безопасность. В общем виде информационную безопасность можно представить как состояние защищенности информационных ресурсов. Но определенная таким образом информационная безопасность может являться объектом и других преступлений УК, поэтому применительно к данной главе под информационной безопасностью следует понимать совокупность общественных отношений, складывающихся в процессе защиты информационных ресурсов, охраны прав пользователей и субъектов информатизации, а также обеспечение безопасности пользования компьютерными системами и сетями. Таким образом, проявляется компьютерный характер охраняемой информации и оборудования, что позволяет отграничить преступления данной главы от других преступлений, воздействующих на информационную безопасность. Поэтому было бы более логичным конкретизировать родовой объект преступлений, содержащихся в главе 31 УК, как безопасность использования компьютерной информации.

Преступления, содержащиеся в главе 28 УК России, направлены против установленного порядка общественных отношений, который регулирует изготовление, использование, распространение и защиту компьютерной информации. Само название главы ориентирует на особенности и характер этой категории преступлений.

Раздел XVI УК Украины определяет родовой объект как отношения, складывающиеся в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей. Следует отметить, что такая трактовка объекта преступных посягательств шире, чем указанные выше. Таким образом, существенные различия проявляются в закреплении законодателями трех славянских государств объекта уголовно-правовой охраны.

Следующее различие можно привести по количеству статей, включенных в Уголовные кодексы стран. Наибольшее количество – семь статей – содержит УК

Беларуси, по три статьи включено в уголовные кодексы России и Украины. Однако, такое различие в количестве не говорит о качественном различии и количество составов преступлений примерно одинаково. Так, ст. 272 УК Российской Федерации (неправомерный доступ к компьютерной информации) сформулирована так, что охватывает своим содержанием такие ст. УК Республики Беларусь, как модификация компьютерной информации, неправомерное завладение компьютерной информацией, компьютерный саботаж. Ст. 349 УК Беларуси (несанкционированный доступ к компьютерной информации), хотя по объективной стороне и схожа со ст. 272 УК России, но отличается по субъективной стороне. Белорусский вариант предусматривает неосторожную форму вины, российский – умышленную. По сути, содержание ст. УК Украины также более широкое и включает в себя несколько составов.

Одинаковыми для трех стран явились преступления, связанные с созданием, распространением или использованием вредоносных программ и нарушением правил эксплуатации компьютерной системы или сети, а вот ответственность за изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети закреплена только в УК Республики Беларусь.

И в заключение будет целесообразно проанализировать размеры и вид наказания, предусмотренные Уголовными кодексами трех стран за вышеуказанные преступления. Спектр видов наказаний за данную группу преступлений примерно одинаков для всех трех стран. К ним относятся: общественные работы (обязательные работы), штраф, лишение права занимать определенные должности или заниматься определенной деятельностью, исправительные работы, арест, ограничение свободы, лишение свободы. Если же говорить о тяжести наказаний, то самым тяжким наказанием для всех стран является лишение свободы, но размер его различается. Более строгое наказание предусмотрено в УК Беларуси – до десяти лет лишения свободы за компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, и за разработку, использование либо распространение вредоносных программ, повлекшие тяжкие последствия. Меньший размер – до пяти лет лишения свободы – предусмотрен на Украине за хищение, присвоение, вымогательство компьютерной информации или завладение ею путем мошенничества или злоупотребления служебным положением, если они причинили существенный вред. В России максимальный срок лишения свободы по этой категории преступлений составляет семь лет за создание, использование либо распространение вредоносных программ для ЭВМ, повлекшие тяжкие последствия.

Таким образом, не смотря на кажущуюся схожесть компьютерных преступлений, закрепленных в Уголовных кодексах Беларуси, России и Украины, имеются некоторые различия, отражающие разные подходы к пониманию этой группы преступлений. И это естественно, поскольку ранее уголовное законодательство не сталкивалось с этой проблемой. Однако изучение и анализ этих различий позволит выработать единые подходы к криминализации общественно-опасных деяний в сфере компьютерных технологий. Унификация норм уголовного законодательства в странах СНГ, предусматривающих ответственность за компьютерные преступления, позволит более эффективно вести борьбу с данной группой преступлений.