УДК 343.2/.7(4/9)

Аратулы К.

Казахский национальный университет имени аль-Фараби,
Республика Казахстан, г. Алматы
E-mail: kunya8585@mail.ru

СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА ЗАРУБЕЖНЫХ СТРАН ОБ ОТВЕТСТВЕННОСТИ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ

В Казахстане работу по выявлению, пресечению и раскрытию киберпреступлений, а также преступлений, совершаемых с использованием информационных технологий, осуществляет созданное в 2003 году в структуре МВД управление «К». Для системной борьбы с информационными преступлениями в 2006 году был создан Национальный контактный пункт по борьбе с преступлениями в сфере информационных технологий, который осуществляет постоянный обмен информацией со странами СНГ и дальнего зарубежья.

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с информационными правонарушениями. Требуется совершенствование процессов и подходов обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с киберпреступностью.

На эффективности противодействия информационной преступности сказывается несовершенство правового обеспечения информационной сферы во многих стран, в том числе и в Казахстане. Но за последние несколько лет Казахстан провел законодательную реформу в сфере урегулирования вопросов, связанных с информационными отношениями, особенно удачно и своевременно криминализированы деяния в Уголовный кодекс РК по ряду норм. Была выделена отдельная глава «Уголовные правонарушения в сфере информатизации и связи» состоящяя из целых 9 отдельных статей от 205-ой по 213 ст.ст. включительно [1]. Хотя некоторые из них отдельно выделенные те же нормы, ранее кодифицированные в статью 227 УК РК 1997 года [2]. Но тем не менее небольшая модификация в составе этих норм произошла. К примеру, «Принуждение к передаче информации» название конечно же имеет неоднозначное понимание, но такие мелкие пробелы в законодательстве могут встречаться, хотя не должны, мы надеемся на ближайшие совершенствоания и дополнения данной главы новыми, общественно необходимыми нормами. Ранее информационные преступления в Казахстане рассматривались в качестве и в составе экономических преступлений, аналогичная же проблема наблюдается и в уголовном законодательстве Узбекистана: состав преступления «Нарушение правил информатизации» (статья 174) отнесен к

преступлениям против собственности и предусмотрен в главе «Хищение чужого имущества» УК Узбекистана [3]. По-разному пределяется родовой объект киберпреступлений в уголовном законодательстве стран СНГ и некоторых государств постсоветского пространства. В Уголовных кодексах России (глава 28, статьи 272-274), Азербайджана (глава 30, статьи 271-273), Кыргызстана (глава 28, статьи 289-291), Туркменистана (глава 33, статьи 333-335), Армении (Раздел 9. Глава 24, статьи 251-257) и Эстонии («Преступления в сфере компьютерной информации», статьи 268-274) в отдельных главах объединены нормы об уголовной ответственности за преступления в сфере компьютерной информации (безопасности компьютерной информации – УК Армении). Уголовное законодательство Республики Беларусь (Раздел XII. Глава 31, статьи 349-355) и Таджикистана (Раздел XII, статьи 298-304) предусматривают в качестве родового объекта киберпреступлений информационную безопасность, объединив общественно опасные деяния в главу (раздел) «Преступления против информационной безопасности». Возникают трудности в определении родового объекта киберпреступлений, подлежащих уголовно-правовой охране по УК Грузии (глава 35. «Компьютерные преступления», статьи 284-286) и Молдовы (глава «Преступления в сфере информатики», статьи 259-261). В УК Украины родовой объект определен как отношения в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей и общественно опасные деяния объединены в разделе XVI. «Преступления в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей» (ст.ст. 361-363, 361-1, 361-2, 361-3) [4]. Во многих европейских старанах (Германия, Франция, Нидерланды, Италия и т.д.) законодательная база также разнобойная, в УК Германии, к примеру есть статья по названием «Информационное мошеничество», то время как в соседней стране во Франции законодательством такое преступное деяние не предусмотрено. Анализ показывает, что национальное уголовное законодательство государств в сфере ответственности за киберпреступления характеризуется относительным разнообразием. Развитие и изменения национального законодательства по борьбе с киберпреступностью в вышеназванных государствах обусловлено появлением и тенденциями киберпреступности и при подробном анализе обнаруживает лишь некоторые закономерности. Совершенствование информационных технологий и проникновение их во все большее количество сфер человеческой жизнедеятельности ведет к возникновению новых форм преступных посягательств и необходимостью выработки эффективных мер борьбы с ними, а это, в свою очередь, к криминализации новых деяний, внесению изменений в уже существующее уголовное законодательство и принятию новых норм. Бесспорно, что эффективное международное сотрудничество в борьбе с киберпреступностью невозможно, если в законодательстве одной страны деяние криминализовано, а в другой – уголовной ответственности не предусмотрено. Отсутствие единообразия в национальном уголовном законодательстве стран может негативно отразиться на развитии методов эффективной борьбы с киберпреступностью – явлением,

для которого не существует государственных границ. Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются киберпреступниками, орудующими в любом месте киберпространства, независимо от юрисдикции государств, имея компьютер и доступ в Интернет. Эффективное противостояние информационной преступности, учитывая ее трансграничный характер, невозможно, если расследование преступлений, выдача правонарушителей, их преследование в суде, затруднены или вообще неосуществимы из-за различия в национальном уголовном законодательстве стран. Фактически, эти различия ограждают киберпреступников от преследования, являясь своеобразным «барьером» для них, позволяют уйти от ответственности, оставляя безнаказанными их деяния. Вследствие этого государства, прилагающие усилия для защиты своих граждан от киберпреступников, тратят их впустую.

С другой стороны, из-за различий уголовно-правового регулирования отношений в сфере информационных технологий, лица, соблюдающие законы своего государства, могут подвергнуться уголовному преследованию в другом. Такая ситуация обосновывает потребность выработки международной стратегии борьбы с киберпреступлениями и унификации национальных законодательств в области уголовно-правового регулирования отношений в сфере информационных технологий.

Приходится признать то, что законодательное регулирование анализируемых отношений в уголовно-правовой сфере отстает от стремительного развития компьютерных информационных технологий. Нынешнее состояние уголовного законодательства об ответственности за киберпреступления, с момента принятия, которого шел непрерывный, стремительный процесс информационного развития человечества, не полным образом отражает глобальных перемен в киберпространстве. Уголовное законодательство недостаточно эффективно регулирует отношения, складывающиеся при совершении информационных преступлений, вследствие чего не реализуются его охранительные и предупредительные функции. Уголовная ответственность в законодательстве Казахстана, как и в законодательстве некоторых государств СНГ, предусмотрена за компьютерные преступления, т.е. за преступления, которые совершаются в отношении компьютеров и компьютерной информации, при этом деяния, которые совершаются с их использованием и посягают на другие объекты уголовно-правовой охраны, остаются вне сферы уголовной ответственности. В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности требуют криминализации ряда современных общественно опасных деяний таких как «Информационное мошеничество», «Распространение СПАМа», «Информационный подлог», «Создание и распространение в сети информационный материал, пропагандирующий и обучающий людей терроризму и экстремизму», «Компьютерный саботаж» и многое другое, что является общественно опасным и отвечает нынешним требованиям информационных отношений в

современных реалиях. Было бы эффективно использовать одни и те же правовые нормы при расследовании и раскрытии информационных правонарушений на отчественном и международном уровне.

Литература

1 Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями на 24.11.2015 г.)

2 Уголовный кодекс Республики Казахстан от 16 июля 1997 года № 167-I (утратил законную силу)

3 Уголовный кодекс Республики Узбекистан от 22 сентября 1994 года № 2012-XII. – www.online.zakon.kz

4 Сборник УК стран СНГ. – www.twirpx.com/law/criminal/foreign/codes/

References

1 The criminal code of the Republic of Kazakhstan of July 3, 2014 No. 226-V (with changes and additions on 11/24/2015)

2 The criminal code of the Republic of Kazakhstan of July 16, 1997 No. 167-_ (I have lost validity)

3 The criminal code of the Republic of Uzbekistan of September 22, 1994 No. 2012-X II. – www.online.zakon.kz

4 Collection of CC of the UIS (Union of the independent states countries). – www.twirpx.com/law/criminal/foreign/codes/