СРАВНИТЕЛЬНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПО ЗАКОНОДАТЕЛЬСТВУ США И СТРАНАХ СНГ

COMPARATIVE AND LEGAL CHARACTERISTICS OF CRIMES IN THE FIELD OF INFORMATION TECHNOLOGIES UNDER THE LEGISLATION OF THE USA AND CIS COUNTRIES

V. Zudaeva

Summary. This article discusses the regulatory framework for information security in the United States and the CIS countries. As well as the approaches of foreign legislators to responsibility for these crimes. The analysis and characterization of regulations governing this area has been carried out.

Keywords: information security, criminal act, information technology, computer crimes.

Зудаева Вероника Вячеславовна
Старший преподаватель, Восточно-Сибирский институт МВД России (г. Иркутск)
veronikaz2007@mail.ru

Аннотация. В данной статье рассматривается нормативно-правовое регулирование информационной безопасности в США и странах СНГ. А так же подходы зарубежных законодателей к ответственности за данные преступления. Проведен анализ и характеристика нормативных актов, регулирующих данную область.

Ключевые слова: информационная безопасность, преступное деяние, информационные технологии, компьютерные преступления.

За последнее время актуальность информационных преступлений значительно возрастает, это связанно с тем, что наука и технологии непрерывно развиваются. Данная проблема достигает больших размеров, она не касается одного города или страны, она касается всех государств и мира в целом. И затрагивает интересы не только частных лиц, но и интересы национальной безопасности.

Принято считать, что информационным преступлением является умышленные преднамеренные действия, направленные на разрушение или хищение информации в информационных сетях и системах, исходящие из хулиганских и корыстных побуждений. Особенностью данных преступлений является то, что они могут совершаться удаленно, из любой точки земного шара и объект посягательства не является материальным, а представлен в цифровом виде, и в случае взлома или кражи происходит не «отнятие» какого-либо предмета, а «копирование», то есть у собственника остается и сохраняется доступ к объекту. И так объектом преступления в сфере информации является общественные отношения, которые связаны с безопасностью информации и систем обработки информационных ресурсов с помощью компьютерной техники. Лица, осуществляющие данные деяния, как и все остальные, привлекаются к уголовной ответственности.

Можно выделить ряд преступлений совершаемых в сфере информации, это:

1. Нелегальный доступ к информационным ресурсам;
2. Создание, распространение и использование вирусов и вирусных программ, наносящих вред технике;
3. Несоблюдение закрепленных правил эксплуатации техники, технологий и информационных систем.

Перечисленные преступления несут в себе угрозу для функционирования и деятельности организаций и компаний, потому как они могут нарушить трудовой процесс автоматизированных систем управления и контроля объектов деятельности, в последующем привести к ошибкам в работе различных систем и технических средств. Информационные преступления тянут за собой негативные последствия в виде физического и материального ущерба, а так же приводят к незаконному искажению, распространению и уничтожению информации. Предлагаем рассмотреть способы защиты информаци-

онных технологий и информации в законодательстве США и стран СНГ.

Итак, законодательство США в сфере информационной безопасности достаточно разнообразно, так как нормативные акты отдельных штатов различаются между собой, и оно составляет совокупность законов, которые создают правовую основу для проведения и формирования государственной политики в сфере информационной безопасности.

Большим преимуществом для законодательной базы США является то, что она уделила немало значения вопросам безопасности в информационных системах государства, противодействия компьютерной преступности, регулирования взаимоотношений в области передачи информации и конфиденциальности частной жизни.

Подвергая рассмотрению нормативную базу законодательства США в сфере информационной защиты, можно сделать выводы о том, что оно направленно на обеспечение граждан правами на информацию и конфиденциальность их частной жизни, а с другой — на безопасность информации, как важной части безопасности государства, то есть он направлен на поддержание уровня баланса интересов как личности, общества, так и государства.

В Америке первым законом, регламентирующим отношения в области информационной защиты, является закон «О защите информации», принятый в 1906 году. В настоящее время основой для формирования и проведения государственной политики США в сфере безопасности информации в интересах обеспечения национальной безопасности государства образуют более 500 федеральных законов и значительное количество законов штатов.

В настоящее время к основным документам, регламентирующим сферу информационной безопасности можно отнести: основные законы, уголовные кодексы штатов, директивы президента США и соответствующие стратегии США.

С возникновением новых информационных технологий и процессов появляется необходимая потребность в их правовом регулировании и защите. Несмотря на то, что право является универсальным регулятором общественных отношений, именно в сфере компьютерной безопасности, страны СНГ не были готовы к их возникновению. Так, рассмотрим законодательство стран СНГ:

В Уголовном кодексе Украины преступления в сфере компьютерной информации отражены в разделе 16 «Преступления в сфере использования электронно-вычислительных машин, систем и компьютерных сетей», он состоит из 3 статей [3].

В Уголовном кодексе Республики Беларусь преступлениям в сфере компьютерной информации посвящен раздел 7, глава 31 «Преступления против информационной безопасности» она состоит из 7 статей [4].

В Уголовном кодексе Республики Казахстан преступления в сфере компьютерной информации отражены в главе 7 «Уголовные правонарушения в сфере информатизации и связи» которая состоит из 9 статей [5].

В Уголовном кодексе Таджикистан преступления в сфере компьютерной информации отражаются в разделе 7, главе 28 «Преступления против информационной безопасности» она состоит из 7 статей [6].

В Уголовном кодексе Российской Федерации преступления в сфере компьютерной информации отражены в главе 28 «Преступления в сфере компьютерной информации» она состоит из 4 статей [7].

Выше была перечислена нормативная база защиты компьютерной информации с помощью общих положений национального уголовного законодательства стран СНГ. Нельзя не согласиться с тем, что решение проблемы компьютерной преступности требует согласованных международных действий и сотрудничества. Ради этой цели 23 ноября 2001 года в Будапеште, была открыта Европейская Конвенция о компьютерных преступлениях. Данная конвенция сыграла не малую роль в формировании современного международного законодательства в информационной сфере. Вместе с тем, конвенция требует создание благоприятных условий для интернет провайдеров, с целью оказания с их стороны помощи и содействия государственным органам со сбором, фиксацией и перехватом необходимой информации. При этом провайдерам следует сохранять полную конфиденциальность о фактах подобного сотрудничества, для безопасности [1].

Преступления в информационном пространстве не имеют определенных территориальных ограничений. Их пресечение и предупреждение требует принятие совместных мер и решений со стороны заинтересованных государств. И одним из первых документов для стран участниц СНГ в борьбе с преступлениями в сфере компьютерной информации является, соглашение подписанное 1 июня 2001 г., которое было подписано всеми участниками содружества стран [2].

Данный документ призывал всех стран к сплоченному взаимодействию, выявлению, раскрытию и пресечению преступлений в сфере компьютерной информации

и принятию мер для эффективной борьбы с данными преступлениями. Соглашение так же стремится к гармонизации законодательства содружества стран в сфере компьютерной преступности.

В заключение всему вышесказанному следует добавить, несмотря на то, что законодательство перечисленных стран стремится урегулировать все общественные отношения, в том числе в сфере компьютерной информации, оно не всегда может прогнозировать развитие техники. Законодательству есть куда стремиться и развиваться. Поэтому потребности противодействия преступности в сфере новейших информационных технологий, защита пользователей информационных систем от мошенничества, обеспечения конфиденциальности информации в информационных системах, защита прав интеллектуальной собственности, определяют необходимость дальнейшего развития и усовершенствования существующего нормативно-правового регулирования информационной безопасности.

ЛИТЕРАТУРА

1. Конвенция Совета Европы о компьютерных преступлениях от 23 ноября 2001 г. URL: http:// conventions.coe.int
2. Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации. URL: http://www.ifap.ru
3. Уголовный кодекс Украины от 5 апреля 2001 года № 2341-III (с изменениями и дополнениями по состоянию на 23.11.2018 г.)
4. Уголовный кодекс Республики Беларусь от 9 июля 1999 года № 275-З (с изменениями и дополнениями по состоянию на 17.07.2018 г.)
5. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 21.01.2019 г.)
6. Уголовный кодекс Республики Таджикистан от 21 мая 1998 года № 574 (с изменениями и дополнениями по состоянию на 02.01.2019 г.)
7. Уголовный кодекс Российской Федерации от 13.06.1996 N63-ФЗ (ред. от 27.12.2018) (с изм. и доп., вступ. в силу с 08.01.2019)
8. Дэвид Эмм. Киберпреступность и закон: обзор положений законодательства США. URL: http://www.securelist.com

Журнал «Современная наука: актуальные проблемы теории и практики»

Г. Иркутск