

Я.С. Лузикова

*УО «Могилевский государственный
университет им. А.А. Кулешова»*

ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ И РЕСПУБЛИКИ БЕЛАРУСЬ

В статье рассматриваются проблемы развития уголовного законодательства Республики Беларусь и Российской Федерации в сфере информационной безопасности.

Развитие информационных технологий в последние несколько лет привело к распространению и увеличению количества преступлений, связанных с информационной безопасностью, и затрагивающих как интересы граждан различных стран, так и самих государств. В связи с увеличением количества данных видов преступлений – законодательства различных стран пополнились статьями, предусматривающими уголовную ответственность за совершение преступлений против информационной безопасности в сфере Интернета.

Так, в Республике Беларусь данная сфера регулируется главой 31 Уголовного кодекса – «Преступления против информационной

безопасности», предусматривающей ответственность за совершение семи различных деяний в данной области. В тоже время уголовное законодательство Российской Федерации определяет данные преступления в главу 28 Уголовного кодекса «Преступления в сфере компьютерной информации», которая содержит три статьи, предусматривающие определенное наказание за совершение деяния.

В Уголовном кодексе Республики Беларусь (далее – УК Республики Беларусь) глава начинается со статьи 349, которая определяет ответственность за несанкционированный доступ к компьютерной информации. В данной статье под несанкционированным доступом к компьютерной информации понимается несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты, повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда [1]. Уголовный кодекс Российской Федерации (далее – УК Российской Федерации) начинается с аналогичной статьи 272, определяющей неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации [2]. Стоит отметить более широкое описание понятия несанкционированного доступа в диспозиции статьи УК Республики Беларусь, что позволяет более точно определить соотношение совершенного деяния к данной статье. В тоже время обязательное наличие последствий в совершенном деянии как в УК Республики Беларусь, так и в УК Российской Федерации указывает на различные методы совершения преступления: изменение, уничтожение, блокирование, вывод из строя компьютерного оборудования в Республике Беларусь и уничтожение, блокирование, модификация либо копирование компьютерной информации в Российской Федерации.

Один из методов совершения преступлений в данной сфере в Российской Федерации, а именно модификация компьютерной информации, в УК Республики Беларусь вынесен в отдельный состав преступления и отражается в статье 350. Данная статья подробно раскрывает понятие модификации компьютерной информации, под которой понимается изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности [1]. Таким образом, можно говорить о более широком определении отдельных видов преступлений против информационной безопасности

для каждого деяния в законодательстве Республики Беларусь и более компактном их выражении в законодательстве Российской Федерации.

Ст.ст. 351-353 УК Республики Беларусь содержат такие составы преступлений, как: компьютерный саботаж, неправомерное завладение компьютерной информацией, изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети. Уголовное законодательство Российской Федерации подобных статей не имеет, что может свидетельствовать о совершенствовании главы 28 УК Российской Федерации с включением в нее новых составов.

Одним из наиболее «популярных» деяний в сфере преступлений против информационной безопасности и преступлений в сфере компьютерной информации является распространение вредоносных программ. Законодательства обоих государств предусматривает наказание за совершение данного преступления. Так, в УК Республики Беларусь деяние регулируется ст. 354, которая включает в данный состав разработку компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработку специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами [1]. Ст. 273 УК Российской Федерации, в свою очередь, говорит о создании, распространении или использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации [2].

Обязательным признаком обоих составов, в данном случае, будет являться цель, которая в большей степени совпадает в двух статьях: несанкционированное уничтожение, блокирование, модификация, копирование компьютерной информации. Статьи как УК Республики Беларусь, так и УК Российской Федерации посвящены нарушению правил эксплуатации компьютерной системы или сети в Республике Беларусь и средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в Российской Федерации.

Ст. 355 УК Республики Беларусь предусматривает ответственность за умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного

оборудования либо причинение иного существенного вреда [1]. В ст. 274 УК Российской Федерации предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб [2]. Уголовным законодательством Республики Беларусь предусмотрено совершение данного деяния специальным субъектом – лицом, имеющим доступ к компьютерной системе или сети, в то время, как законодательство Российской Федерации данный элемент не предусматривает. Несмотря на данное различие, законодательство обоих государств в качестве обязательного признака предусматривает последствия, но главным отличием составов будет совершение деяния, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации в законодательстве Республики Беларусь и отсутствие неосторожности в составе, предусмотренном законодательством Российской Федерации.

Также стоит отметить, что глава 28 УК Российской Федерации с 1 января 2018 года была дополнена статьей 274¹, предусматривающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации [2]. В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» под критической информационной инфраструктурой понимаются «объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». Данным законом также раскрывается понятие объектов критической информационной инфраструктуры, то есть информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектов критической информационной инфраструктуры. Таким образом, в уголовное законодательство данного государства будет включена абсолютно новая статья, прямо регулирующая широкий круг общественных отношений, которые косвенно регулируются законодательствами других стран.

Говоря о схожести законодательства в данной сфере, регулирующей преступления против информационной безопасности и компьютерной информации, стоит отметить наличие статей как в УК Республики Беларусь, так и Российской Федерации, регулирующих схожий круг общественных отношений. Но, несмотря на схожесть отдельных статей уголовного законодательства соседних государств, они остаются

обособленными элементами, взаимодействующими на уровне принятия совместных нормативных правовых актов об оказании сотрудничества в данной сфере. По нашему мнению, уголовному законодательству Российской Федерации не хватает более четкого отграничения составов преступлений в сфере компьютерной информации, а также наличие отдельных статей, посвященных определенному кругу общественных отношений для более полного соотношения деяния по составу. При этом стоит отметить появление статьи в российском законодательстве, регулирующей совершенно новые общественные отношения в сфере критической информационной инфраструктуры. Таким образом, можно говорить о потребности для законодательства Республики Беларусь принять решение о необходимости внедрения в свое законодательство статьи, регулирующей такие общественные отношения, а для Российской Федерации – необходимости расширения главы, предусматривающей ответственность за совершение преступлений в сфере компьютерной информации.

Список использованных источников

1. Уголовный кодекс Республики Беларусь [Электронный ресурс]: 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г.

: одоб. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 18.07.2017 г. // Эталон. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2018.

2. Уголовный кодекс Российской Федерации [Электронный ресурс]: 13.06.1996г., № 63-ФЗ: принят Государственной думой 24 мая 1996г. : одоб. Советом Федерации 5 июня 1996 года г. : в ред. Федерального закона от 19.02.2018 г. // СПС КонсультантПлюс. – Дата доступа: 10.04.2018 г.

The article is devoted to the problems of development of criminal legislation of the Republic of Belarus and the Russian Federation in the field of information security.