Published in the Slovak Republic
Vestnik policii
Has been issued since 2014.
E-ISSN: 2414-0880
2019, 6(2): 76-80

DOI: 10.13187/vesp.2019.2.76
www.ejournal21.com

Cybercrime Counteraction: Comparative Analysis of Criminal Laws of Russia and Belarus

Victor Vorobyov [a, *]

[a] Syktyvkar State University, Russian Federation

Abstract

Crime in the field of computer information tends to grow steadily and affects the most important areas of activity not only of individual States, but also of the world community as a whole. In this regard, the improvement of legislation to combat these criminal attacks becomes extremely urgent.

In Russia and the Republic of Belarus, criminal legislation in the field of combating computer crimes has a number of significant differences, which can include: various lists of computer crimes; Different content of similar offences; The lack of legal interpretation of certain terms contained in the articles; Features of the characterization of individual crimes; Some inconsistency between the criminal laws of these countries and the model criminal code of the CIS member States.

In addition, the differences concerning the subjective side of the investigated types of crimes can be considered significant, when in the legislation of one country liability occurs only if the consequences are careless, and in the other - the form of guilt can be both intentional and careless.

Keywords: computer crimes, criminal liability, information security.

1. Введение

Развитие информационных технологий породило новое криминальное явление – компьютерная преступность (киберпреступность). Появление новых видов преступлений требует постоянного совершенствования не только программно-технических средств противодействия и защиты информации, но и совершенствование законов в сфере борьбы с этими проявлениями преступности.

2. Материалы и методы

Сравнительный анализ уголовных кодексов российской Федерации и Республики Беларусь позволил выявить ряд существенных отличий в определении места этих деяний в системе уголовных законов и перечне компьютерных преступлений, а также в описании сходных составов преступлений.

Приведенные автором данные Международного союза электросвязи при ООН по уровню компьютерной безопасности в России и Беларуси за последние годы подкрепляю выводы о наличии проблем в этой области правоохранительной деятельности.

Синтез, обобщение и аналогия, как методы познания, позволили выявить ряд схожих и отличительных черт исследуемых уголовных законов, которые носят порой существенный

* Corresponding author
E-mail addresses: vorobvv@gmail.com (V. Vorobyov)

характер. Некоторым из этих отличий даны авторские оценки, которые позволят в будущем рекомендовать законодателям усовершенствовать уголовные кодексы этих стран.

3. Обсуждение

Весной 2019 года Международный союз электросвязи при ООН опубликовал предварительный отчет «Глобальный индекс кибербезопасности». Согласно данному отчету, Россия занимает 28 позицию в рейтинге стран по уровню кибербезопасности, а Беларусь находится на 74 месте. Нижнюю позицию рейтинга среди стран СНГ занял Кыргызстан, расположившись на 129 месте. В пятерку же лидеров вошли Великобритания, США, Франция, Литва и Эстония (Global Cybersecurity Index, 2019).

В уголовном законодательстве Российской Федерации компьютерные преступления содержатся в главе 28 «Преступления в сфере компьютерной информации», которая входит в раздел IX «Преступления против общественной безопасности и общественного порядка.

В УК РФ компьютерные преступления, входящие в главу 28 условно можно разделить на три группы: неправомерный доступ к охраняемой законом компьютерной информации (ст. 272); незаконное обращение с вредоносными программами (ст. 273); нарушение правил эксплуатации компьютеров (ст. 274).

Судебная статистика в РФ свидетельствует о достаточно низком уровне противодействия киберпреступности. Так, в 2014 году к уголовной ответственности по ст. 272 УК РФ было привлечено 180 человек, в 2015 – 206, 2016 – 147, 2017 – 134, 2018 – 119 и в первом полугодии 2019 года – 58. По 273 статье УК РФ в 2014 году к уголовной ответственности привлекалось 214 человек, 2015 – 248, 2016 – 182, 2017 – 196, в 2018 – 124 и в первом полугодии 2019 – 48. С применение статьи 274 УК РФ существует ряд проблемных вопросов, о чем свидетельствуют данные статистики. По данной статье уголовное преследование в 2014 году не осуществлялось, в 2015 – лишь в отношении 2-х человек, 2016 – тоже 2-х, 2017 – 0, 2018 – в отношении 1-го человека, в первом полугодии 2019 – не один человек не был привлечен к уголовной ответственности (Data of judicial statistics, 2020).

Указанная глава в конце 2017 года была дополнена статьей 274[1], которая устанавливает ответственность за неправомерное воздействие на критическую информационную структуру Российской Федерации. Данный состав мы не стали выделять как отдельный вид компьютерного преступления, так как информация, циркулирующая в критической информационной структуре, фактически может быть приравнена к охраняемой законом компьютерной информации, а способы неправомерного, деструктивного воздействия на нее существенно не отличаются от приведенной выше классификации. По данной статье в 2018 уголовному преследованию ни кто не подвергался.

Ответственность за неправомерный доступ к компьютерной информации наступает лишь в отношении охраняемой законом компьютерной информации, например, государственной или коммерческой тайне, тайне частной жизни и иной информации которая охраняется законами России.

Уголовная ответственность за неправомерный доступ по УК РФ наступает лишь в тех случаях, когда информация была уничтожена, заблокирована, модифицирована или скопирована. Таким образом, факт ознакомления с информацией без деструктивного воздействия на неё или копирования, уголовно-правовых последствий не влечет.

Также наступление последствий в виде уничтожения, блокирования или модификации информации является обязательным условием привлечения к уголовной ответственности за оконченное преступление, ответственность за которое предусмотрена ст. 274 УК РФ. При этом еще должен быть причинен крупный ущерб.

По ст. 273 УК РФ уголовная ответственность наступает за создание, использование или распространение вредоносных программ, независимо от наступления каких-либо последствий. Причинение крупного ущерба или наступление тяжких последствий предусмотрены в квалифицированных составах этой статьи. Оно влечет более стогую ответственность.

Отличительной особенностью уголовного закона Беларуси является то, что глава 31 «Преступления против информационной безопасности» находится в одноименном разделе № 12. Мы видим, что законодатель не нашел аргументов в пользу того, что информационные преступления относятся какой-либо укрупненной группе преступлений.

Полагаем, что это наиболее перспективный подход, так как открывает возможность развиваться этой главе с учетом появления новых технологий и новых видов преступлений в этой сфере (Criminal code of the Republic of Belarus, 1999).

Содержание норм главы 31 УК РБ во многом совпадают с нормами об ответственности за компьютерные преступления в других странах-участниках СНГ, но при этом довольно сильно отличается от норм об ответственности за компьютерные преступления в российской Федерации. Так, в главу 31 входят составы, в которых предусмотрена уголовная ответственность за несанкционированный доступ к компьютерной информации (ст. 349), модификацию компьютерной информации (ст. 350), компьютерный саботаж (ст. 351), неправомерное завладение компьютерной информацией (ст. 352), изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (ст. 353), разработка, использование либо распространение вредоносных программ (ст. 354) и нарушение правил эксплуатации компьютерной системы или сети (ст. 355).

Ответственность за несанкционированный доступ к компьютерной информации наступает лишь в случае, если это сопровождалось нарушением системы защиты и если наступили по неосторожности неблагоприятные последствия в виде изменение, уничтожение, блокирование информации либо причинение иного существенного вреда. Здесь мы наблюдаем такой же подход к формулированию субъективной стороны этого состава, как и в УК Армении, где ответственность на неправомерный доступ наступает при неосторожной форме вины по отношению к наступающим последствиям.

В квалифицированных составах установлена более строгая ответственность за преступление, совершённое из корыстных побуждений или в составе группы лиц. Особенно интересно содержание части 3 ст. 349 УК РБ, в которой субъектами могут выступать лица не только неправомерно получившие доступ к информации, но и имеющие доступ к компьютерной системе и самовольно воспользовались компьютером, средствами связи компьютерной системы или сети, если это повлекло по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия.

Считаем важным отметить положительный опыт указания в норме не просто абстрактной фразы «иные тяжкие последствия», как это указано в УК РФ, а когда перечисляются наиболее характерные последствия, которые следует относить к тяжким. Такой подход исключает излишний объем усмотрения при решении вопроса о квалификации деяния со стороны правоприменителя.

За модификацию компьютерной информации предусмотрена ответственность в составе ст. 350 УК Беларуси. В уголовных кодексах стран-участниц СНГ имеются похожие преступления, однако, их названия отличаются. Так, в УК Азербайджана такое преступление именуется как фальсификация компьютерных данных (ст. 273-2), а в УК Армении – как изменение компьютерной информации (ст. 252). В УК России модификация, рассматривается лишь как одно из последствий неправомерного доступа к охраняемой законом компьютерной информации (ст. 272).

Модификацией признается изменение информации либо внесение в компьютерную систему заведомо ложной информации, если это причинило существенный вред. При этом в норме имеется оговорка, которая исключает наличие признаков преступления против собственности. Эта оговорка обоснована наличием в УК Беларуси ст. 212, предусматривающей ответственность за хищение имущества путем изменения компьютерной информации, либо путем введения в компьютерную систему ложной информации. Таким образом, в уголовном законе исключена конкуренция норм.

В части 2 этой статьи предусмотрено наказание за модификацию информации, если это повлекло по неосторожности тяжкие последствия, в том числе крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде.

Компьютерный саботаж (ст. 351), то есть умышленные уничтожение, блокирование компьютерной информации или программы, либо вывод из строя компьютерного оборудования или машинного носителя.

Статьи о компьютерном саботаже примерно этого же содержания можно увидеть в уголовных кодексах Кыргызской Республики (ст. 306), Республики Таджикистан (ст. 300), Республики Узбекистан (ст. 278-5) и Республики Армения (ст. 253).

Надо отметить, что в компьютерном саботаже законодатели Беларуси и некоторых из перечисленных выше стран не стали ограничиваться только воздействием на информацию в виде уничтожения, блокирования или привидения ее в негодность, но и включил сюда разрушительное воздействие, как на аппаратную часть компьютерных систем, так и на машинные носители.

Компьютерный саботаж, сопряженный с несанкционированным доступом, либо повлекший тяжкие последствия является квалифицированным составом, из чего следует вывод, что в ч.1 ст. 351 УК РБ субъектом выступает лицо, которое имело право доступа к компьютерной информации.

Под неправомерным завладением компьютерной информацией в ст. 352 УК РБ понимается несанкционированное копирование либо иное неправомерное завладение компьютерной информацией, либо перехват информации, передаваемой с использованием средств компьютерной связи. При этом состав преступления будет образовываться лишь при наступлении существенного вреда.

Такая формулировка объективной стороны этого преступления представляется весьма удачной, так как в отличии от уголовного кодекса Российской Федерации, суть преступления не ограничивается только копированием компьютерной информации, но и предполагает любое другое завладение информацией, в том числе и путем ее перехвата, например, распечатка информации на бумажный носитель, фотографирование с экрана, перехват через Wi-Fi сети и т.п.

Следует обратить внимание и на отсутствие в УК РБ указания на то, что информация должна быть охраняемой законом. По-видимому, это компенсируется тем, что этот состав сконструирован как материальный и преступление будет окончено, только если наступит существенный вред.

Как и в некоторых других странах-участниках СНГ (Таджикистан, Узбекистан, Украина, Молдова, Армения, Азербайджан, в УК РБ имеется состав, предусматривающий ответственность за изготовление с целью сбыта либо сбыт специальных программ или аппаратных средств для осуществления неправомерного доступа к компьютерной информации. При этом, в УК РБ эта информация должна находиться в защищенной компьютерной системе или сети (ст. 353).

Уголовное законодательство Республики Беларусь пошло иным путем и предусмотрело отдельный состав преступления (ст. 354) о создании, использовании или распространении вредоносных либо специальных вирусных программ. Аналогичным образом составы о незаконном обращении с вредоносными программами были включены в уголовные кодексы Туркменистана, Кыргызстана, Таджикистана, Узбекистана, Казахстана и Армении. Однако, составы об ответственности за незаконный оборот вредоносных программ и составы, предусматривающие наказание за создание специальных программных и технических средств для совершения компьютерных преступлений есть только в УК Таджикистана и УК Узбекистана.

Отдельного внимания заслуживает подход, продемонстрированный в уголовном кодексе Украины, где указанные нормы объединены в одну статью и объективная сторона включают в себя, как создание, использование и распространение вредных программ, так и технических устройств для несанкционированного вмешательства в работу компьютеров. Данный подход нам представляется весьма универсальным и заслуживающим внимания для целей совершенствования отечественного уголовного закона.

В завершении гл. 31 УК РБ находится состав ст. 355 (нарушение правил эксплуатации компьютерной системы или сети), то есть, умышленное нарушение правил эксплуатации компьютерной системы, повлекшее по неосторожности уничтожение, блокирование или модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда.

Следует отметить, что в Российской Федерации данный состав преступления практически не работает и судебная статистика свидетельствует о единицах привлеченных к уголовной ответственности лиц, совершивших это деяние (2016 году привлечено 2 человека, в 2017 – 0, а в 2018 лишь 1 человек привлечен по ст. 274 УК РФ).

Причинами такой низкой эффективности отдельной нормы уголовного кодекса стала неопределённость в понимании термина «правила эксплуатации». В российском

законодательстве отсутствует какой-либо нормативный акт, в котором бы было разъяснено, что понимать под правилами эксплуатации средств обработки компьютерной информации и какие руководящие акты к ним относить.

Таким образом, сравнительно-правовой анализ отдельных норм об ответственности за компьютерные преступления в России и Республике Беларусь свидетельствует об отсутствии какой-либо единой логики, что, конечно же, препятствует эффективному взаимодействию в борьбе с этим видом криминального проявления, как на межгосударственном, так и на национальном уровне.

References

Data of judicial statistics – Data of judicial statistics for 2014–2019 [Electronic resource]. URL: https://http://www.cdep.ru/index.php?id=79

Global Cybersecurity Index, 2019 – Global Cybersecurity Index (2019). [Electronic resource]. URL: http://www.tadviser.ru/index.php/Статья:Глобальный_индекс_кибербезопасности_Global_Cybersecurity_Index_(GCI)

Criminal Code of Armenia – Criminal Code of Armenia (2003). [Electronic resource]. URL: https://www.unodc.org/res/cld/document/armenia_criminal_code_html/Armenia_Criminal_Code_of_the_Republic_of_Armenia_2009.pdf

Criminal code of the Republic of Belarus – Criminal code of the Republic of Belarus, 1999 [Electronic resource]. URL: http://www.pravo.by/document/?guid=3871&p0=Hk9900275

Противодействие киберпреступности: сравнительный анализ уголовных законов России и Беларуси

Виктор Воробьев [a, *]

[a] Сыктывкарский государственный университет, Российская Федерация

Аннотация: Преступность в сфере компьютерной информации имеет тенденцию к устойчивому росту и затрагивает важнейшие сферы деятельности не только отдельных государств, но и мирового сообщества в целом. В связи с этим, исключительно актуальным становится совершенствование законодательства о противодействии этим преступным посягательствам.

В России и Республике Беларусь уголовное законодательство в сфере борьбы с компьютерными преступлениями имеет ряд существенных отличий, к которым можно отнести: различные перечни компьютерных преступлений; различное содержание сходных по названию составов преступлений; отсутствие легального толкования некоторых терминов, содержащихся в статьях; особенности квалификации отдельных преступлений; некоторая несогласованность уголовных законов этих стран с модельным уголовным кодексом государств – участников СНГ.

Кроме этого существенными можно считать отличия, касающиеся субъективной стороны исследуемых видов преступлений, когда в законодательстве одной страны ответственность наступает лишь при неосторожном отношении к наступающим последствиям, а в другой – форма вины может быть как умышленной, так и неосторожной.

Ключевые слова: компьютерные преступления, уголовная ответственность, информационная безопасность.

* Корреспондирующий автор
Адреса электронной почты: vorobvv@gmail.com (В. Воробьев)