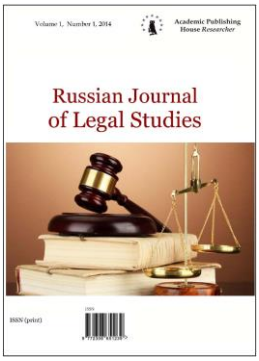
Published in the Slovak Republic
Russian Journal of Legal Studies
Has been issued since 2014.
E-ISSN: 2413-7448
2018, 5(1): 49-57

DOI: 10.13187/rjls.2018.1.49
www.ejournal25.com



Computer Crimes as a Part of Information Crime in Russia: Problems of Counteraction

Victor V. Vorobyov [a, *]

[a] Syktyvkar State University, Russian Federation

Abstract

Crime in the sphere of computer information tends to steady growth and mentions the major fields of activity not only the certain states, but also the world community in general. In this regard, exclusively relevant is an improvement of the legislation on counteraction to these criminal encroachments.

By the analysis, logical and comparative and legal methods of knowledge it was revealed that the Russian criminal legislation in the sphere of fight against computer crimes has a number of essential shortcomings to which it is possible to carry: lack of legal interpretation of many terms which are contained in articles 159.3, 159.6, 187, 272, 273, 274 Criminal Code of the Russian Federation; shortcomings of designs of these articles; inconsistency of the Russian criminal legislation with the international legal acts and also shortcomings of the international cooperation in counteraction of computer crime.

The data of judicial statistics on convicts provided by the author in Russia for commission of computer crimes from 2003 for 2017 I support conclusions about existence of problems in this area of law-enforcement activity.

Synthesis, generalization and analogy as knowledge methods, allowed to give author's definition to such concepts as: "illegal access to computer information"; "malicious computer application". For the purpose of improvement of the criminal legislation of Russia, offers on introduction of additions in article 272-273 of the Criminal Code of the Russian Federation are made and also new Art. 274.1 of UKRF is subject to the critical analysis.

Keywords: computer crimes, illegal access to computer information, the malicious computer application, service regulations of means of storage, processing or transfer of computer information, fraud in the sphere of computer information, crime counteraction.

1. Введение

Развитие информационных технологий породило такое криминальное явление как компьютерная преступность. Эти преступления затрагивают практически все сферы жизни человека, где присутствуют информационные технологии. Появление новых видов преступлений неразрывно связано с естественным прогрессом в этой области, что, естественно, требует постоянного совершенствования не только технических и программных средств противодействия, но и законодательного регулирования в сфере борьбы с компьютерными преступлениями.

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

2. Материалы и методы

К основным методам данного исследования относятся анализ, логический и сравнительно-правовой метод, синтез, обобщение и аналогия.

В настоящей работе были использованы научные труды таких исследователей как В.В. Крылов, А.Л. Осипенко, Е.И. Панфилова, А.С. Попов, А.В. Сизов, В.П. Числин. Подвергнуты детальному анализу статьи Уголовного кодекса РФ, международные соглашения по вопросам борьбы с компьютерной преступностью, материалы судебной практики и судебной статистики в части привлечения к уголовной ответственности за совершение преступлений в сфере информационно-коммуникационных технологий.

3. Обсуждение

В уголовном законодательстве РФ предусмотрена ответственность за такие виды компьютерных преступлений как неправомерный доступ к компьютерной информации (ст. 273 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) и нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Кроме этого в УК РФ имеются такие составы преступления, как мошенничество с использованием платежных карт (ст. 159.3), мошенничество в сфере компьютерной информации (ст. 159.6), неправомерный оборот средств платежей (ст. 187). Эти составы в России принято относить к преступлениям в сфере информационно-коммуникационных технологий.

Несмотря на предпринимаемые законодателем и правоприменителем меры, в 2017 году число преступлений в России в сфере информационно-телекоммуникационных технологий увеличилось с 65 949 до 90 587. Их доля от числа всех зарегистрированных в России преступных деяний составляет 4,4 % – это почти каждое 20 преступление. Самыми распространенными киберпреступлениями являются неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ). Если в 2017 году зарегистрировано 1 883 таких преступлений (+7,7 %), то за первое полугодие 2018 года – 1 233 (+3,4 %). Наибольшее их количество выявлялось в 2017 году в Удмуртской Республике (194), Коми (132), Омской (75), Владимирской (66), Кировской (64), Волгоградской областях (60), Москве (60), Краснодарском крае (51) (Коми, 2018).

Данные судебной статистики в Российской Федерации свидетельствуют о том, что число лиц, осужденных за преступления в сфере компьютерной информации до 2010 года увеличивалось, а начиная с 2011 года стало уменьшаться. Так в 2003 году за преступления, предусмотренные статьями 272-274 УК РФ число осужденных составило 152 человека, в 2004 – 137, в 2005 – 203, в 2006 – 191, в 2007 – 241, в 2008 – 257, в 2009 – 347, в 2010 – 321, в 2011 – 258, в 2012 – 280, в 2013 – 268, в 2014 – 218, в 2015 - 235, в 2016 – 185 и в 2017 году – 202 человека (Data of judicial statistics).

Такое малое количество осужденных по ст. 272-274 УК можно объяснить тем, что согласно статистике правоохранительных органов России в более чем 50 % возбужденных уголовных дел отсутствуют подозреваемые. А при расследовании мошенничеств в сфере компьютерной информации (ст. 159.6 УК), лишь в 1 % возбужденных уголовных дел есть подозреваемые.

По сравнению с 2016 годом в 2017 году на 19,6 % уменьшилось количество расследованных преступлений по указанным статьям (с 903 до 726), при этом выросло на 30,5 % (с 790 до 1031) число нераскрытых преступлений. Раскрываемость данных преступлений составила 41,3 %.

Судебная статистика, также свидетельствует о том, что Российское правосудие относится к компьютерным преступникам достаточно лояльно. Так, только в 2015 году к реальному лишению свободы были осуждены лишь 5 человек, из них до 1-го года осуждено 4 человека, а до 2-х лет – 1 человек. Условно к лишению свободы были осуждены 42 человека. К ограничению свободы – 43, исправительным работам – 5 и к штрафу осуждены 12 человек. А по амнистии от наказания за совершение компьютерных преступлений в 2015 году было освобождено 122 осужденных.

Кроме этого следует отметить и то, что даже когда лица привлечены к уголовной ответственности и им назначено, как видно, достаточно мягкое наказание, вопрос возмещения причиненного преступлением материального вреда остаётся актуальным. В среднем по данным преступлениям потерпевшим возмещается только 10-20 % материального вреда. Это, от части, вызвано как пробелами в законодательстве, так и недоработками правоохранительных органов, для которых первоочередной задачей является раскрытие преступления, а соблюдение материальных прав потерпевшего вторично, а порой совсем не важно.

В законодательстве России вопросы уголовного преследования и вопросы материального возмещения причиненного ущерба, в целом, разделены. Суд рассматривает вопросы причастности и виновности лица, вид и размер наказания. Несмотря на то, что уголовно-процессуальным законодательством РФ в целях защиты и восстановления материальных прав потерпевшего предусмотрена процедура рассмотрения гражданского иска в уголовном процессе (ст. 44 УПК РФ), судьи по уголовным делам, не желая рассматривать гражданские иски, направляют потерпевших в гражданский суд, у которого другое процессуальное законодательство, сроки, порядок обжалования, затраты на юридическую помощь и т.п.

Таким образом, для лиц, склонных и/или способных к совершению компьютерных преступлений создается ситуация практически безнаказанности за совершаемые преступные деяния. Тот, кто был привлечены к такой мягкой ответственности, вряд ли исправится. Он лишь будет более изощренным и осторожным при совершении преступлений в будущем.

Анализ отдельных составов хотелось бы начать со статьи 272 УК РФ.

Обязательными признаками этого преступления являются:

1) деяние, которое состоит в неправомерном доступе к охраняемой законом компьютерной информации;

2) последствия в виде уничтожения, блокирования, модификации или копирования компьютерной информации;

3) причинно-следственная связи между совершенным деянием и наступившими последствиями.

Отсутствие хотя бы одного из перечисленных признаков исключает уголовную ответственность за оконченное преступление, либо свидетельствует, о том, что было покушение или приготовление к этому преступлению.

Понятие «неправомерный доступ к охраняемой законом компьютерной информации» в законодательстве, науке и в практике трактуется по-разному, что, конечно же, нельзя оставлять без внимания и необходимо попытаться сформулировать унифицированное определение этого понятия.

Приведем примеры различного толкования термина «доступ к информации» в некоторых нормативных актах РФ:

1. Так, согласно п. 6 ст. 2 ФЗ «Об информации, информационных технологиях и о защите информации» доступ к информации – это возможность получения информации и ее использования;

2. Закон РФ «О государственной тайне» (ст. 2) доступ к сведениям, составляющим государственную тайну, трактует как санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну;

3. Федеральный закон «О коммерческой тайне» (п. 5 ст. 3) доступ к информации, составляющей коммерческую тайну определяет как ознакомление определенных лиц с информацией, составляющей коммерческую тайну, с согласия ее обладателя или на ином законном основании при условии сохранения конфиденциальности этой информации;

4. В Соглашении о сотрудничестве государств – участников СНГ в борьбе с преступлениями в сфере компьютерной информации 2001 г. неправомерный доступ сформулирован как несанкционированное обращение к компьютерной информации (Cooperation agreement, 2001).

В Российской науке, также наблюдается разность подходов к определению этого термина. Однако, весь спектр точек зрения Российских ученых-правоведов можно свести

к двум принципиальным позициям: первая заключается в том, что под доступом следует понимать получение возможности манипулировать информацией (копировать, модифицировать, уничтожать и т.п.) (Панфилова, Попов, 1998: 28); вторая – под доступом следует понимать не только получение возможности манипулировать информацией, но и простое ознакомление с ней без всякого воздействия (Числин, 2004: 13-14; Крылов, 1998: 28; Сизов, 2009: 32-35).

С учетом представленных точек зрения и положений нормативных актов, под неправомерным доступом к компьютерной информации предлагается понимать несанкционированное обращение к компьютерной информации, дающее возможность получить или ознакомиться с информацией, использовать эту информацию, воздействовать на неё. Однако принятие данного определения за основу требует внесения изменений в диспозицию ст. 272 УК. Здесь следует согласиться с А.Л. Осипенко и к числу альтернативных последствий добавить «получение и/или ознакомление с информацией» (Осипенко, 2007: 43-47).

Защищенность информации программными или техническими средствами не является обязательным признаком состава преступления, предусмотренного ст. 272 УК РФ, иначе это неоправданно сузило бы действие этой статьи. Достаточно и того, что информация защищена законом.

Оконченным преступление будет считаться только при наступлении, указанных в ст. 272 УК последствий в виде уничтожения, блокирования, модификации либо копирования охраняемой законом компьютерной информации.

В составе ст. 273 УК РФ законодатель установил ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Вредоносная программа является ключевым понятием, содержащимся в диспозиции ст. 273 УК РФ. Этот термин имеет как доктринальное, так и нормативное толкование.

Представляется, что вредоносность программы заключается не только и не столько в способности уничтожать, блокировать, модифицировать или копировать информацию (это рабочие функции многих программ), а в том, что они выполняют эти функции помимо воли, согласия (санкции) собственника или другого законного владельца информации (Воробьев, 2015а: 54-58).

В российском уголовном праве наблюдается некоторая разница во мнениях по определению понятия «вредоносная программа», однако, принципиально отличающихся точек зрения не встречается. Аналогичная ситуация складывается и в нормативно-правовом толковании этого термина.

В Соглашении о сотрудничестве государств - участников в борьбе с преступлениями в сфере компьютерной информации указано, что вредоносная программа – это созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

Дискуссионным остается один вопрос – с какого момента считать создание вредоносной программы оконченным преступлением? Когда программа находится в электронном виде и способна осуществлять вредоносные функции, или же можно признавать вредоносной программой и текст программы, представленный в любой материальной форме, в том числе в виде записи на бумажном носителе?

В ст. 1261 ГК РФ установлено, что программой для ЭВМ является представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств в целях получения определенного результата, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения.

Таким образом, возникает ситуация, при которой норма ГК РФ не соответствует положениям уголовного законодательства РФ. Противоречие состоит в том, что в уголовном праве есть такие понятия, как приготовление к преступлению и покушение на преступление (ст. 30 УК РФ). Учитывая содержание этих понятий, создание исходных подготовительных

материалов в ходе разработки программы следует квалифицировать как покушением на преступление (покушение на создание вредоносной программы). В связи с этим, подготовительные материалы, полученные в ходе разработки компьютерной программы, и порождаемые ею аудиовизуальные отображения в контексте данного преступления не могут признаваться компьютерной программой.

Следует пояснить, что положения ст. 1261 ГК не оспариваются, поскольку эта норма регулирует вопросы защиты авторских прав на компьютерные программы, в связи с чем такое определение компьютерной программы вполне оправданно. Вместе с тем, применение его по аналогии в этом случае было бы не верным.

Вышеизложенное приводит к выводу о необходимости закрепления в примечании к ст. 273 УК РФ определения такого понятия как «вредоносная компьютерная программа». Так, под вредоносной компьютерной программой предлагается понимать компьютерную программу, заведомо предназначенную для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации, ознакомления с ней или нейтрализации средств защиты компьютерной информации.

Следует отметить, что распространение исходных текстов вредоносных компьютерных программ, несомненно, имеет общественную опасность и по этому, наряду с распространением вредоносных программ, статья должна быть дополнена распространением исходных текстов вредоносных программ.

Нами ранее отмечалось, что вредоносная программа не является предметом преступления, так как именно она оказывает на него вредоносное воздействие. В связи с этим представляется, что вредоносная компьютерная программа не является факультативным признаком объекта преступления состава ст. 273 УК РФ, а выступает в качестве продукта преступной деятельности, который следует относить к объективной стороне состава преступления (Воробьев, 2015b: 92-100).

По своей конструкции состав является формальным и преступление признается оконченным в момент создания, распространения или использования вредоносной компьютерной программы независимо от момента наступления последствий.

В УК РФ отсутствует ответственность за приобретение и/или хранение вредоносных программ с целью их использования и/или распространения. В вязи с чем, представляется необходимым, наряду с имеющимся перечнем деяний, дополнить данную статью такими действиями, как приобретение и/или хранение вредоносной компьютерной программы или ее исходных текстов с целью окончательного создания, использования и/или распространения этой программы.

Анализ судебной практики свидетельствует о том, что подавляющее большинство раскрытых преступлений, предусмотренных ст. 273 УК РФ были совершены не профессиональными хакерами или программистами, а обычными пользователями компьютеров. Наиболее типичными преступлениями этого вида являются: копирование и использование вредоносных программ, блокирующих работу веб-ресурсовили отдельных компьютеров, принадлежащих гражданам; копирование и использование вредоносных программ, перехватывающих трафик и собирающих такие данные как логины и пароли; копирование, использование и распространение вредоносных программ, предназначенных для активации контрафактных программных продуктов, путем нейтрализации средств их защиты.

Намного реже привлекаются лица, обладающие навыками программирования и самостоятельно создающие вредоносные компьютерные программы.

Чаще всего эти преступления совершаются из хулиганских или корыстных побуждений, и, как правило, квалифицируются по совокупности со ст. 146 УК РФ (Нарушение авторских и смежных прав), реже со ст. 159.6 (Мошенничество в сфере компьютерной информации).

Статьей 274 УК РФ предусмотрена 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, если это причинило кому либо крупный ущерб.

Нарушение правил эксплуатации может выражаться как в полном игнорировании, так и в ненадлежащем соблюдении правил. Нарушение может быть выражено в форме действия или бездействия (совершение запрещенных действий или невыполнение виновным действий, предписанных правилами). Термины «нарушение» и «несоблюдение» правил, в контексте данной статьи, следует рассматриваться как равнозначные (синонимы).

Основной проблемой применения данной нормы является отсутствие какой-либо официальной системы правил и инструкций в компьютерной сфере и по этому на протяжении последних 20 лет действия Уголовного кодекса РФ эта норма практически не применялась.

Серьезным шагом на пути борьбы с компьютерными преступлениями явилось принятие Федерального закона от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». В связи с принятием этого закона в УК РФ была введена новая статья 274.1 (Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации). Данная статья предусматривает ответственность:

- за создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации (ч. 1 ст. 274.1);
- за неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 2 ст. 274.1);
- за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации (ч. 3 ст. 274.1).

Максимальное наказание за эти преступления составляет до 6 лет лишения свободы, а при наступлении тяжких последствий – до 10 лет лишения свободы.

Представляется, что российский законодатель мог бы обойтись внесением соответствующих дополнений в статьи 272-274 УК РФ, так как новая статья 274.1 УКРФ практические их дублирует с одним лишь дополнением «информации, содержащейся в критической информационной инфраструктуре Российской Федерации». Достаточным было бы закрепить этот признак в качестве квалифицирующих обстоятельств в статьях 272-273 УК РФ.

Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» определены субъекты критической информационной инфраструктуры. В их числе: государственные органы, государственные учреждения, российские юридические лица и (или) индивидуальные предприниматели, которым на праве собственности, аренды или на ином законном основании принадлежат информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сфере здравоохранения, науки, транспорта, связи, энергетики, банковской сфере и иных сферах финансового рынка, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности, российские юридические лица и (или) индивидуальные предприниматели, которые обеспечивают взаимодействие указанных систем или сетей (п. 8 ст. 2).

В связи с участившимися случаями компьютерных атак на государственные учреждения, крупные корпорации и банки, необходимость принятия этих изменений в законодательстве России давно назрела, а об их эффективности можно будет судить лишь через время.

Участие России в международно-правовом механизме борьбы с киберпреступностью, к сожалению, носит региональный, а не глобальный характер. Россия активно участвует в формировании международного законодательства в рамках СНГ, однако не участвует в единственном на сегодняшний день Европейском международном соглашении о противодействии киберугрозам - Конвенции Совета Европы о преступности в сфере компьютерной информации (ETS № 185), заключенной в г. Будапеште в 2001 году (Convention, 2001).

Этому, конечно, есть объяснения. Первое - Конвенция не решает вопросов юрисдикции расследования трансграничных киберпреступлений того или иного государства, ограничиваясь общими положениями. По-прежнему не урегулированы уголовно-процессуальные вопросы. Этому способствует и то, что до настоящего времени идут дискуссии о критериях определения места совершения компьютерного преступлений, когда затронуты несколько государств. Второе - Конвенция содержит нормы, противоречащие, по мнению России, её интересам. Так Конвенция, позволяет правоохранительным органам, с добровольного согласия лица, имеющего полномочия раскрыть информацию, получать доступ к компьютерным данным, находящимся на территории другого государства, без согласования с компетентными властями государства, что ограничивает действие принципа национального суверенитета при расследовании преступлений.

4. Результаты

Таким образом, в свете постоянно растущего уровня киберугроз, который наблюдается в последние годы, низкого уровня борьбы с компьютерными преступлениями в Российской Федерации возникла острая необходимость дальнейшего совершенствования национального законодательства, а также скорейшего разрешения имеющихся противоречий в международных отношениях по вопросам борьбы с компьютерными преступлениями.

5. Заключение

В России необходимо продолжать совершенствовать уголовное законодательство в сфере борьбы с компьютерными преступлениями.

России нельзя ограничиваться международным сотрудничеством только в рамках СНГ. Необходимо, пусть и с оговорками, входить в Конвенцию Совета Европы о преступности в сфере компьютерной информации.

Литература

Воробьев, 2015a – *Воробьев В.В.* О содержании объективной стороны состава статьи 273 УК РФ (создание, использование и распространение вредоносных компьютерных программ) // *Управленческие аспекты развития северных территорий России: Всероссийская научная конференция (20-23 октября 2015 г., Сыктывкар) в 4* ч. Сыктывкар: ГОУ ВО КРАГСиУ. Ч. 1, 2015.

Воробьев, 2015b – *Воробьев В.В.* Вредоносные компьютерные программы в уголовном законодательстве Российской Федерации // *Путеводитель предпринимателя. Научно-практическое издание: Сборник научных трудов. Вып. XXVI* / под научной ред. Л.А. Булочниковой. М.: Российская академия предпринимательства; Агентство печати «Наука и образование», 2015.

Панфилова, Попов, 1998 – *Панфилова Е.И., Попов А.С.* Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» / под ред. Б.В. Волженкина. СПб.: СПб. юрид. ин-т Ген. Прокуратуры, 1998.

Коми, 2018 – Коми вошла в топ-5 регионов по количеству киберпреступлений, 2018. [Электронный ресурс]. URL: https://www.bnkomi.ru/data/news/82355

Крылов, 1998 – *Крылов В.В.* Криминалистические проблемы оценки преступлений в сфере компьютерной информации // Уголовное право, 1998. № 3.

Осипенко, 2007 – *Осипенко А.* Уголовная ответственность за неправомерный доступ к конфиденциальной компьютерной информации // Уголовное право, 2007. № 3.

Сизов, 2009 – *Сизов А.В.* Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право, 2009. № 1.

Числин, 2004 – *Числин В.П.* Уголовно-правовые меры защиты информации от неправомерного доступа. Автореф. … канд. юр. н. М.: Института международного права и экономики им. А.С. Грибоедова, 2004.

Data of judicial statistics – Data of judicial statistics [Elektronnyi resurs]. URL: http://www.cdep.ru/index.php?id=79 (date of access 20.08.2017). [in Russian]

The cooperation agreement – The cooperation agreement of the State Parties of the Commonwealth of Independent States in fight against crimes in the sphere of computer information (2001). [Elektronnyi resurs]. URL: http://www.pravo.gov.ru [in Russian]

Convention, 2001 – Convention of the Council of Europe on crime in the sphere of computer information (2001) [Elektronnyi resurs]. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185

References

Vorob'ev, 2015a – *Vorob'ev, V.V.* (2015). O soderzhanii ob"ektivnoi storony sostava stat'i 273 UK RF (sozdanie, ispol'zovanie i rasprostranenie vredonosnykh komp'yuternykh programm) [Maintenance of the objective side of structure of article 273 Criminal Code of the Russian Federation (creation, use and distribution of malicious computer applications)]. *Upravlencheskie aspekty razvitiya severnykh territorii Rossii: Vserossiiskaya nauchnaya konferentsiya (20-23 oktyabrya 2015 g., Syktyvkar) v 4 ch.* Syktyvkar: GOU VO KRAGSiU. Ch. 1.

Vorob'ev, 2015b – *Vorob'ev, V.V.* (2015). Vredonosnye komp'yuternye programmy v ugolovnom zakonodatel'stve Rossiiskoi Federatsii [Malicious computer applications in the criminal legislation of the Russian Federation]. Putevoditel' predprinimatelya. Nauchno-prakticheskoe izdanie: Sbornik nauchnykh trudov. Vyp. XXVI. Pod nauchnoi red. L.A. Bulochnikovoi. M.: Rossiiskaya akademiya predprinimatel'stva; Agentstvo pechati «Nauka i obrazovanie».

Panfilova, Popov, 1998 – *Panfilova, E.I., Popov, A.S.* (1998). Komp'yuternye prestupleniya: Seriya «Sovremennye standarty v ugolovnom prave i ugolovnom protsesse» [Computer crimes: «The Modern Standards in Criminal Law and Criminal Trial»]. Pod red. B.V. Volzhenkina. SPb.: SPb. yurid. in-t Gen. Prokuratury.

Komi, 2018 – Komi voshla v top-5 regionov po kolichestvu kiberprestuplenii [Komi has entered in top-5 regions by the number of cybercrimes], 2018. [Elektronnyi resurs]. URL: https://www.bnkomi.ru/data/news/82355

Krylov, 1998 – *Krylov, V.V.* (1998). Kriminalisticheskie problemy otsenki prestuplenii v sfere komp'yuternoi informatsii [Criminalistic problems of assessment of crimes in the sphere of computer information]. *Ugolovnoe pravo,* № 3.

Osipenko, 2007 – *Osipenko, A.* (2007). Ugolovnaya otvetstvennost' za nepravomernyi dostup k konfidentsial'noi komp'yuternoi informatsii [Criminal liability for illegal access to confidential computer information]. *Ugolovnoe pravo,* № 3.

Sizov, 2009 – *Sizov, A.V.* (2009). Nepravomernyi dostup k komp'yuternoi informatsii: praktika pravoprimeneniya [Illegal access to computer information: practice of law enforcement]. *Informatsionnoe pravo,* № 1.

Chislin, 2004 – Chislin, V.P. (2004). Ugolovno-pravovye mery zashchity informatsii ot nepravomernogo dostupa [Criminal and legal measures of protection of information from illegal access]. Avtoref. ... kand. yur. n. M.: Instituta mezhdunarodnogo prava i ekonomiki im. A.S. Griboedova.

Data of judicial statistics – Data of judicial statistics [Elektronnyi resurs]. URL: http://www.cdep.ru/index.php?id=79 (date of access 20.08.2017). [in Russian]

The cooperation agreement – The cooperation agreement of the State Parties of the Commonwealth of Independent States in fight against crimes in the sphere of computer information (2001). [Elektronnyi resurs]. URL: http://www.pravo.gov.ru [in Russian]

Convention, 2001 – Convention of the Council of Europe on crime in the sphere of computer information (2001) [Elektronnyi resurs]. URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185

Компьютерные преступления как часть информационной преступности в России: проблемы противодействия

Виктор Викторович Воробьев [a, *]

[a] Сыктывкарский государственный университет им. Питирима Сорокина,
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.

Путем анализа, логического и сравнительно-правового методов познания было выявлено, что российское уголовное законодательство в сфере борьбы с компьютерными преступлениями имеет ряд существенных недостатков, к которым можно отнести: отсутствие легального толкования многих терминов, содержащихся в статьях 159.3, 159.6, 187, 272, 273, 274 УК РФ; недостатки в конструкциях этих статей; несогласованность российского уголовного законодательства с международными правовыми актами, а также недостатки международного сотрудничества в области противодействия компьютерной преступности.

Приведенные автором данные судебной статистики по осужденным в России за совершение компьютерных преступлений за период с 2003 по 2017 годы подкрепляю выводы о наличии проблем в этой области правоохранительной деятельности.

Синтез, обобщение и аналогия, как методы познания, позволили дать авторское определение таким понятиям как: «неправомерный доступ к компьютерной информации»; «вредоносная компьютерная программа». С целью совершенствования уголовного законодательства России, сделаны предложения по внесению дополнений в статьи 272-273 УК РФ, а также подвержена критическому анализу новая ст. 274.1 УКРФ.

Ключевые слова: компьютерные преступления, неправомерный доступ к компьютерной информации, вредоносная компьютерная программа, правила эксплуатации средств хранения, обработки или передачи компьютерной информации, мошенничество в сфере компьютерной информации, противодействие преступности.

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