Published in the Slovak Republic
Zhurnal grazhdanskogo i ugolovnogo prava
Has been issued since 2014.
E-ISSN: 2413-7340
2019, 6(1): 25-33

DOI: 10.13187/zngup.2019.1.25
http://ejournal22.com

Some Problems on the Fight against Cybercrimes in the Russian Federation

Victor V. Vorobyov [a, *]

[a] Syktyvkar State University, Russian Federation

Abstract

Crime in the sphere of computer information tends to increases steadily and affects the most important areas of activity of not only individual states but the global community as a whole. In this connection, improving of the legislation for counteraction against these criminal attempts becomes an urgent task of today.

Through analysis, logical and comparative-legal methods of cognition, it has been found that the Russian criminal legislation in the sphere of struggling cybercrime has a number of fundamental defects, among them: the lack of legal interpretation of many terms in Articles 159.3, 159.6, 187, 272, 273, 274 of the Criminal Code of the RF; faults in the structure of these Articles; incompliance of the Russian criminal legislation with the international legal acts, as well as faults in international cooperation in the sphere of cybercrime counteraction.

The data of court statistics on the convicted for cybercrimes in Russia from 2003 till 2016 substantiate the conclusions on the presence of certain problems in this sphere of law enforcement activity.

The cognition methods of synthesis, summarizing and analogy enabled to give the author's definition to such notions as "illegal access to computer information" and "harmful software". To improve the Russian criminal legislation, we propose amendments to Articles 272-273 and criticize the new Article 274.1 of the Russian Criminal Code.

The materials of the research can be useful for law-makers, scholars of legal disciplines, personnel of the law enforcement bodies, judges of criminal courts, professors and students of law faculties.

Keywords: Cybercrime; illegal access to computer information; harmful software; rules of exploitation of facilities for storing, processing or transmitting the computer information; fraud in the sphere of computer information; counteraction against crime.

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

В настоящей работе были использованы научные труды таких исследователей как М.В. Богомолов, 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.

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

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.

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, и за первое полугодие 2016 года – 68 человек (Данные судебной статистики ...).

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.

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. При этом по амнистии от наказания за совершение компьютерных преступлений в 2015 году было освобождено 122 осужденных (Данные судебной статистики ...).

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. Уголовный суд рассматривает вопросы причастности и виновности лица, вид и размер наказания. Несмотря на то, что в ст. 44 УПК в целях защиты и восстановления материальных прав потерпевшего предусмотрена процедура рассмотрения гражданского иска в уголовном процессе, судьи по уголовным делам, не желая рассматривать гражданские иски, направляют пострадавшую

сторону в гражданский суд, у которого, в свою очередь, 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. Те, кто и были привлечены к такой сравнительно мягкой ответственности, вряд ли исправятся, а лишь будут более изощренными и осторожными при совершении преступлений в будущем.

Анализ отдельных составов, хотелось бы начать со статьи 272 УК РФ, который предусматривает ответственность за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

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.

Неправомерный доступ к компьютерной информации совершается только путем действия.

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

Приведем примеры толкования термина «доступ к информации» в различных нормативных актах:

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

3. Федеральный закон «О коммерческой тайне» 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 (п. 5 ст. 3);

4. В Соглашении о сотрудничестве государств - участников СНГ в борьбе с преступлениями в сфере компьютерной информации (вступило в силу для России с 17.10.2008) неправомерный доступ сформулировано как несанкционированное обращение к компьютерной информации.

В науке также наблюдается разность подходов к определению этого термина. Однако весь спектр точек зрения ученых можно свести к двум принципиальным позициям. 1) Под доступом следует понимать получение возможности манипулировать информацией (копировать, модифицировать, уничтожать и т.п.). 2) Доступ – это не только получение возможности манипулировать информацией, но и простое ознакомление с ней без всякого воздействия (Богомолов, 2002; Крылов, 1998; Сизов, 2009; Числин, 2004).

Мне думается, под неправомерным доступом нужно 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).

Защищенность информации программными или техническими средствами не является обязательным признаком состава преступления по 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 качестве примера такого преступления можно привести уголовное дело в отношении жительницы города Москвы, которая, имея неприязненные отношения к своей знакомой, заведомо зная адрес электронного почтового ящика и фамилию матери потерпевшей, вход в который защищен «Паролем», желая причинить потерпевшей моральный вред, провела операцию по восстановлению пароля, путем ответа на секретный вопрос. Виновная зашла на почтовый сервер, ввела в поле «Имя» – адрес её электронного почтового ящика и, используя операцию восстановления «Пароля», ответив на секретный вопрос – «Фамилия матери», тем самым неправомерно получила доступ к охраняемой законом компьютерной информации, хранящейся в электронном почтовом ящике. После этого она скопировала из электронного почтового ящика три личные фотографии. Далее виновная неправомерно заменила - секретный вопрос – на «Любимая книга», изменила «Пароль» доступа к указанному электронному почтовому ящику. Тем самым виновная совершила копирование охраняемой законом компьютерной информации, модифицировала и блокировала доступ к электронному почтовому ящику потерпевшей, чем причинила последней моральный вред.

В итоге суд приговорил виновную к небольшому штрафу.

Приведенный пример демонстрирует относительно безобидный вид компьютерного взлома, но в истории компьютерной преступности есть более глобальные и опасные взломы.

Так, в 2004 году у компании Microsoft были украдены 31 тысяча файлов и 13,5 миллионов строк исходного кода Windows 2000. Ни специалистам из Microsoft, ни ФБР так и не удалось найти виновников преступления.

Американец Гонсалес в 2009 году провел серию атак на Heartland Payment System и похитил данные десятков миллионов кредитных карт, а также взломал сети TJX Cos, Bj'S Wholesale Club и Barnes & Noble. Данные с карточек он перепродавал через созданную им группу ShadowCrew. Альберто Гонсалес был приговорен к 20 годам лишения свободы (Досье на Хакера…).

Компьютерные взломы совершаются как отдельными гражданами, так и организованными группами, в том числе международными. Одной из наиболее известных международных хакерских групп является. В 2010 году Anonymous организовала акцию «Возмездие», в рамках которой атаковала системы Visa, PayPal и MasterCard из-за того, что те отказались проводить платежи сайта WikiLeaks (Anonymous: los enemigos de los enemigos…). Через год хакеры поддержали движение против социального неравенства под кодовым названием «Захвати Уолл-Стрит» и обрушили сайт Нью-Йоркской биржи. В 2012 году хакеры из этой группировки провели крупную DDoS-атаку на Европарламент (Хакеры атаковали сайт…). В этом же году «Anonymous» вывели из строя официальный сайт Ватикана (Vatican confirms second Anonymous…). Во время украинского кризиса совершили атаки на сайты российских СМИ и правительственных структур России (10 знаменитых хакерских атак…).

В 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, 2015a).

В 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.

Так, в Соглашении о сотрудничестве государств - участников Содружества Независимых Государств (СНГ) 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 лишь один вопрос – с какого момента считать создание вредоносной программы оконченным преступлением? Когда программа находится в электронном виде и способна осуществлять вредоносные функции, или же возможно 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 не соответствует основным положениям УК. В уголовном праве России есть понятия приготовления и покушения (ст. 30 УК РФ). Учитывая их содержание, 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 РФ не оспариваются, так как эта норма регулирует вопросы защиты авторских прав на компьютерные программы, в связи, с чем такое определение компьютерной программы вполне оправданно, однако, применение его по аналогии в этом случае было бы неверным.

Вышеизложенное приводит нас к выводу о необходимости закрепления в примечании к ст. 273 УК РФ определения такого понятия как «вредоносная компьютерная программа». Я предлагаю под ней 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.

Представляется, что вредоносная программа не является предметом преступления, поскольку 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).

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

В УК 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 непрофессиональными хакерами или программистами, а обычными пользователями компьютеров.

Наиболее типичными преступлениями этого типа являются: копирование и использование вредоносных программ, блокирующих работу веб-ресурсов (как правило, государственных учреждений) или 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. Поэтому на протяжении последних 20 лет действия УК 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).

Представляется, что законодатель мог бы обойтись внесением соответствующих дополнений в статьи 272-274 УК РФ. 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 УКРФ.

Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации» определены субъекты критической информационной инфраструктуры. Это 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 носит региональный, а не глобальный характер. Россия активно участвует в формировании международного законодательства в рамках СНГ. Однако Россия – не член Конвенции Совета Европы о преступности в сфере компьютерной информации 2001 г.

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. 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

Результатом проведенного автором анализа статей УК РФ были выявлены особенности уголовного законодательства в сфере борьбы с компьютерными преступлениями. Сравнительно правовой метод, аналогия и синтез позволили обнаружить отличительные черты российского и международного законодательства в этой области. При обобщении и логическом сопоставлении Российского законодательства и результатов его применения с зарубежными и международными правовыми актами удалось определить пути совершенствования отечественного уголовного закона в сфере борьбы с компьютерными преступлениями.

5. Заключение

Таким образом, 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. России нельзя ограничиваться международным сотрудничеством только в рамках СНГ, нужно, пусть и с оговорками, но не лишающими смысла сотрудничества, входить в Конвенцию Совета Европы о преступности в сфере компьютерной информации (ETS № 185), заключенной в г. Будапеште в 2001 году.

References

10 znamenitykh khakerskikh atak... – 10 znamenitykh khakerskikh atak [10 famous hacker attacks]. [Elektronnyi resurs]. URL: http://masterok.livejournal.com/3346475.html (data dostupa 20.08.2017).

Anonymous: los enemigos de los enemigos... – Anonymous: los enemigos de los enemigos de Wikileaks. [Elektronnyi resurs]. URL: http://blogs.elpais.com/trending-topics/2010/12/quien-es-anonymous.html (data dostupa 20.08.2017).

Bogomolov, 2002 – *Bogomolov M.V.* (2002). Ugolovnaya otvetstvennost' za nepravomernyi dostup k okhranyaemoi zakonom komp'yuternoi informatsii [Criminal liability for illegal access to computer information protected by law]. Krasnoyarsk, P. 68.

Chislin, 2004 – *Chislin V.P.* (2004). Ugolovno-pravovye mery zashchity informatsii ot nepravomernogo dostupa [Criminal-legal means of protecting information from illegal access]. Avtoref. ... kand. yur. n. M.: Instituta mezhdunarodnogo prava i ekonomiki im. A.S. Griboedova, pp. 13-14.

Dannye sudebnoi statistiki... – Dannye sudebnoi statistiki [Data of court statistics]. [Elektronnyi resurs]. URL: http://www.cdep.ru/index.php?id=79 (data dostupa 20.08.2017).

Dos'e na Khakera... – Dos'e na Khakera: Al'bert Gonsales. 20 let tyur'my i 170 000 000 ukradennykh kreditnykh kart. [Elektronnyi resurs]. URL: https://habrahabr.ru/company/edison/blog/315388/ (data dostupa 20.08.2017).

Khakery atakovali sait... – Khakery atakovali sait Evroparlamenta [Hackers attacked web-site of Euro parliament]. [Elektronnyi resurs]. URL: https://lenta.ru/news/2012/01/26/europarl/ (data dostupa 20.08.2017).

Krylov, 1998 – *Krylov V.V.* (1998). Kriminalisticheskie problemy otsenki prestuplenii v sfere komp'yuternoi informatsii [Criminalistic issues of estimating crimes in the sphere of computer information]. *Ugolovnoe pravo,* № 3. P. 84.

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. pp. 43-47.

Panfilova, Popov, 1998 – *Panfilova E.I., Popov A.S.* (1998). Komp'yuternye prestupleniya: Seriya «Sovremennye standarty v ugolovnom prave i ugolovnom protsesse» ["Modern standards in criminal law and criminal procedure" series]. Pod red. B.V. Volzhenkina. SPb.: SPb. yurid. in-t Gen. prokuratury. P. 28.

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. pp. 32-35.

Vatican confirms second Anonymous... – Vatican confirms second Anonymous hack. [Elektronnyi resurs]. URL: http://www.zdnet.com/article/vatican-confirms-second-anonymous-hack-10025615/?tag=mncol%253Btxt (data dostupa 20.08.2017).

Vorob'ev, 2015a – *Vorob'ev V.V.* (2015). Vredonosnye komp'yuternye programmy v ugolovnom zakonodatel'stve Rossiiskoi Federatsii [Harmful software in the criminal legislation of the Russian Federation]. Putevoditel' predprinimatelya. Nauchno-prakticheskoe izdanie: Sb. nauch. trudov. Vyp. XXVI. Pod nauchnoi red. L. A. Bulochnikovoi. M.: Rossiiskaya akademiya predprinimatel'stva; Agentstvo pechati «Nauka i obrazovanie», pp. 92-100.

Vorob'ev, 2015b – *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) [On the content of objective part of corpus delicti by 273 CC RF (creating, using and distributing of harmful software)]. Upravlencheskie aspekty razvitiya severnykh territorii Rossii: Vserossiiskaya nauchnaya konferentsiya (s mezhdunarodnym uchastiem) (20-23 oktyabrya 2015 g., Syktyvkar) v 4 ch. Syktyvkar: GOU VO KRAGSiU, Ch. 1. pp. 54-58.

Некоторые проблемы борьбы с компьютерными преступлениями в Российской Федерации

Виктор Викторович Воробьёв [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

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

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 2016 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.

Материалы данной статьи могут быть полезными для законотворцев, исследователей-правоведов, сотрудников правоохранительных органов, судей по уголовным делам, преподавателей и студентов-юристов.

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.