На правах рукописи

Степанов-Егиянц Владимир Георгиевич

МЕТОДОЛОГИЧЕСКОЕ И ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В РОССИЙСКОЙ ФЕДЕРАЦИИ (УГОЛОВНО-ПРАВОВОЙ АСПЕКТ)

Специальность 12.00.08 – «Уголовное право и криминология; уголовно-исполнительное право»

Автореферат
диссертации на соискание ученой степени
доктора юридических наук

Москва – 2016

Работа выполнена в федеральном государственном бюджетном образовательном учреждении высшего образования «Московский государственный университет имени М.В.Ломоносова», юридический факультет

Научный консультант: **Комиссаров Владимир Сергеевич**
доктор юридических наук, профессор, заведующий кафедрой уголовного права и криминологии

Официальные оппоненты: **Гладких Виктор Иванович,**
доктор юридических наук, профессор, заслуженный юрист Российской Федерации, ФГБОУ ВО «Государственный университет управления», заведующий кафедрой уголовно-правовых дисциплин

Лопатина Татьяна Михайловна,
доктор юридических наук, профессор, ФГБОУ ВО «Смоленский государственный университет», кафедра права.

Чупрова Антонина Юрьевна,
доктор юридических наук, профессор, ФГБОУ ВО «Всероссийский государственный университет юстиции (РПА Минюста России)», кафедра уголовного права и криминологии.

Ведущая организация: Федеральное государственное автономное образовательное учреждение высшего образования «Казанский (Приволжский) федеральный университет».

Защита диссертации «13» сентября 2016 г. в 15 часов 00 минут на заседании диссертационного совета Д 501.001.73 на базе федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» по адресу: 119991, Москва, ГСП-1, Ленинские горы, д.1, строение13-14, (4 гуманитарный корпус), юридический факультет, ауд.535а.

С диссертацией и авторефератом можно ознакомиться в отделе диссертаций научной библиотеки федерального государственного бюджетного образовательного учреждения высшего образования «Московский государственный университет имени М.В. Ломоносова» по адресу: Москва, 119992, Ломоносовский проспект, 27, Фундаментальная библиотека, сектор А, 8 этаж, комната 812 и на сайте www.istina.msu.ru

Автореферат разослан «__» _____ 2016 г.

Ученый секретарь
диссертационного совета А.А. Арутюнян

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования. Начало XXI столетия характеризуется новой политико-экономической и технологической ситуацией, в которой оказалась Россия, активно и последовательно отстаивающая свои национальные интересы в глобальном мире. В круг данных интересов входит и участие России в информационных процессах, что самым тесным образом связано с проблемами обеспечения безопасности государства, общества, субъектов хозяйствования, каждой отдельной личности в информационной сфере.

Развитие и совершенствование правового регулирования общественных, в том числе информационных, отношений, повышение их эффективности – одна из важнейших задач, стоящих перед юридической наукой. Особую актуальность проблемы совершенствования правового регулирования приобретают в наши дни в связи с интенсивным развитием современного информационного общества и высоких технологий.

Отрасль информационных технологий является одной из наиболее динамично развивающихся отраслей, как в мире, так и в России. Объем мирового рынка информационных технологий оценивается в 1,7 трлн. долларов США. Мировой опыт показывает, что конкурентоспособность национальной экономики в целом связана с развитием информационных технологий. По данным Всемирного экономического форума, индекс конкурентоспособности экономики государств имеет высокий уровень корреляции с индексом развития в странах информационно-коммуникационных технологий[1].

Международный союз электросвязи в отчете за 2015 год сообщил, что количество пользователей сети Интернет на Земле выросло до 3,2 миллиарда человек. За прошедшие 15 лет количество людей, которые пользуются сетью,

[1] Распоряжение Правительства РФ от 01.11.2013 № 2036-р «Об утверждении Стратегии развития отрасли информационных технологий в Российской Федерации на 2014 - 2020 годы и на перспективу до 2025 года» // СЗ РФ. 2013. № 46. Ст. 5954.

увеличилось в восемь раз[2]. В России количество Интернет-пользователей в 2015 году составило 84 млн. человек, а уровень проникновения Интернета среди населения России в возрасте от 16 лет достиг показателя 70,4.%[3]

В современных условиях все более актуальными становятся вопросы правового обеспечения безопасного оборота компьютерной информации, как в национальном, так и в международном масштабе. Общественные отношения, возникающие в процессе формирования и использования информационных ресурсов, а также создания, сбора, обработки, хранения, поиска, распространения и предоставления пользователям компьютерной информации, нуждаются в правовом регулировании и охране. В текущих условиях исследование вопросов уголовно-правового противодействия компьютерным преступлениям имеют большое теоретическое и практического значение.

Привлекательность информационных технологий для преступников заключается, прежде всего, в массовости аудитории потенциальных жертв, территориальной удаленности жертвы и преступника, круглосуточности преступного воздействия, отсутствии непосредственного контакта между потенциальной жертвой и преступником, больших возможностях по сокрытию следов преступных действий, а также обеспечении значительного временного разрыва между началом активных действий и наступлением последствий[4].

Уголовная ответственность за совершение преступлений в сфере компьютерной информации в нашей стране была введена с принятием Уголовного кодекса Российской Федерации 1996 года (далее – УК РФ). Глава 26 УК РФ именуется «Преступления в сфере компьютерной информации» и с момента своего вступления в силу вплоть до настоящего времени содержит три состава: ст. 272 (неправомерный доступ к компьютерной информации), ст. 273

---

[2] Международный союз электросвязи [Электронный ресурс]. – Режим доступа: http://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx. Дата обращения: 22.09.2015.

[3] Агентство Интерфакс [Электронный ресурс]. – Режим доступа: http://www.interfax.ru/russia/491974. Дата обращения: 29.12.2015.

[4] Аналитическая справка к заседанию коллегии МВД России 26 сентября 2014 г. по вопросу «О совершенствовании деятельности по раскрытию и расследованию преступлений, совершенных с использованием современных информационных технологий» [Электронный ресурс]. – Режим доступа: https://mvd.ru/mvd/structure1/Departamenti/Organizacionno_analiticheskij_departamen/Novosti._Publikacii._Vistuplenija./item/2298580/?print=1. Дата обращения: 16.02.2015.

(создание, использование и распространение вредоносных компьютерных программ) и ст. 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей).

По данным Министерства внутренних дел РФ в 2006 г. было зарегистрировано 8889 преступлений в сфере компьютерной информации (7337 – ст. 272 УК РФ, 1549 – ст. 273 УК РФ и 3 – ст. 274 УК РФ); в 2007 г. – 7236; в 2008 г. – 9010; в 2009 г. – 11636; в 2010 г. – 7398; в 2011 г. – 2698; в 2012 г. – 2820; в 2013 г. – 2563; в 2014 г. – 1739; в 2015 г. – 2382 (1396 – ст. 272 УК РФ, 974 – ст. 273 УК РФ, 12 – ст. 274 УК РФ)[5].

Данные цифры показывают, что с 2011 г. наблюдается трехкратное снижение числа регистрируемых преступлений по сравнению с показателями 2006 г. Данная статистика при лавинном нарастании количества пользователей компьютеров в нашей стране непосредственно указывает на масштабную латентизацию данного вида преступлений[6]. До 90% преступлений в сфере компьютерной информации остаются латентными.

Общее число выявленных лиц, совершивших компьютерные преступления, также снижалось в период с 2010-2014 гг. В основном это было характерно для неправомерного доступа к компьютерной информации (ст. 272 УК РФ): за пять лет число выявленных лиц, совершивших данное преступление компьютерное преступления, сократилось с 3973 до 290 (то есть более чем в 13 раз) [7].

Интересно отметить, что Бюро специальных технических мероприятий (далее – БСТМ) МВД России указывает, что 2015 г. в России было зарегистрировано 11 тыс. преступлений в сфере и компьютерной информации. Подобное расхождение с данными официальной статистики МВД вызвано тем, что к категории компьютерных преступлений сотрудники БСТМ МВД относят не только деяния, предусмотренные главой 28 УК РФ, но и такие преступления,

---

[5] Министерство внутренних дел [Электронный ресурс]. – Режим доступа: https://mvd.ru/folder/101762.html. Дата обращения: 19.10.2015.

[6] Кривенцов П.А. Латентная преступность России: криминологическое исследование: дис. … канд. юрид. наук: 12.00.08 / Кривенцов Павел Алексеевич – М., 2014. – 124 с.

[7] Криминология. Особенная часть: в 2 т.: учебник для академического бакалавриата / под ред. О. С. Капинус. — М. : Издательство Юрайт, 2016. – Т. 2. С.241.

как кража (ст. 158 УК РФ) мошенничество в сфере компьютерной информации (ст. 159.6 УК РФ), неправомерный оборот средств платежей (ст. 187 УК РФ), а также изготовление и оборот материалов или предметов с порнографическими изображениями несовершеннолетних (ст. 242.1 УК РФ).

В числе тенденций компьютерной преступности отмечается, что все большее число «традиционных» составов преступлений, давно известных уголовному праву, постепенно перемещается в сферу компьютеров и их сетей. Некоторое время назад трудно было представить причинение вреда здоровью или даже убийство человека через сеть Интернет. В настоящее время существует реальная возможность совершения подобных действий, так как, например, современные кардиостимуляторы являются компьютерными устройствами, имеют программное обеспечение, позволяя осуществлять дистанционное программирование и передачу информации. Неправомерный беспроводной доступ в систему управления кардиостимулятора и изменение параметров его работы может привести к вреду здоровью или смерти человека. В этой связи особенно важно определить круг преступлений, относящийся к преступлениям в сфере компьютерной информации, отграничив их от традиционных преступных деяний могут совершаться с использованием компьютеров.

Защита информационного пространства России от современных угроз – это одно из приоритетных направлений обеспечения национальной безопасности, а надежная работа информационных ресурсов, систем управления и связи имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова.

Соответственно, четкое правовое регулирование информационной сферы и безопасной деятельности в сфере использования компьютерной информации выступает залогом эффективного использования информационного фактора в обеспечении развития Российской Федерации и предупреждения возможных негативных влияний на государство и общество, на каждого конкретного

человека, включенного в те или иные информационные правоотношения.

Приведенные сведения дают основания утверждать, что в настоящее время проблемы уголовно-правового регулирования безопасности компьютерной информации являются чрезвычайно актуальными, поскольку от их решения, в том числе, зависит общественный порядок Российской Федерации, национальная безопасность государства, личная безопасность граждан, бесперебойная работа объектов критической инфраструктуры и безопасность компьютерной информации.

Цель и задачи диссертационного исследования. Целью данной диссертационной работы является решение крупной теоретической и прикладной проблемы методологического и законодательного обеспечения безопасности компьютерной информации с помощью уголовно-правовых средств.

В данном исследовании достижение поставленных целей обеспечивалось путем решения следующих взаимосвязанных задач:

– теоретически обосновать необходимость повышенной уголовно-правовой защиты компьютерной информации;

– проанализировать используемый в доктрине уголовного права и законодательстве Российской Федерации понятийный аппарат преступлений против компьютерной информации;

– разработать методологическую базу научных исследований вопросов обеспечения безопасности компьютерной информации;

– определить компьютерную информацию как предмет преступных посягательств;

– провести анализ конституционно-правовых основ борьбы с преступлениями против компьютерной информации;

– рассмотреть международно-правовые основы борьбы с преступлениями против компьютерной информации;

– дать общую характеристику преступлений против компьютерной информации в теории уголовного права Российской Федерации;

– проанализировать уголовно-правовую характеристику составов преступлений против компьютерной информации по уголовному законодательству Российской Федерации;

– классифицировать виды преступных посягательств против компьютерной информации;

– рассмотреть вопросы отграничения преступлений против компьютерной информации от иных преступных посягательств;

– определить пути и способы совершенствования уголовно-правовой защиты компьютерной информации в Российской Федерации.

– разработать комплекс изменений и дополнений в действующий УК Российской Федерации.

Объект и предмет исследования. Объектом диссертационного исследования являются общественные отношения, определяющие комплекс теоретических проблем уголовного права, а также лежащие в основе норм уголовного законодательства, устанавливающих ответственность за преступлениями против компьютерной информации, и практики их применения.

Предмет исследования составляет доктрина уголовного законодательства, комплекс правовых норм уголовного и иного законодательства, обеспечивающих безопасность компьютерной информации, практика квалификации преступлений против компьютерной информации, зарубежный и отечественный опыт борьбы с преступлениями в данной сфере информационных правоотношений.

Методология и методика исследования. При написании диссертационной работы применялись различные методы научного исследования. При этом использовались методы, которые были выбраны с учетом определенных целей и задач, а также объекта и предмета исследования. На различных этапах исследования применялись: общенаучный диалектический метод научного познания действительности, а также специальные методы – историко-правовой, статистический, системно-

структурный, метод моделирования, обобщения и др. Все указанные методы использовались в системной взаимосвязи, что способствовало достижению всесторонности, полноты и объективности научного поиска, конкретности, обоснованности и согласованности сформулированных выводов.

Общенаучный диалектический метод был использован, чтобы понять взаимосвязь тех или иных явлений, определить направление развития существующих отношений в определенной сфере, а также судить о степени прогресса или регресса.

Историко-правовой метод был использован при исследовании генезиса развития вопросов безопасности, эволюцию подходов к ее обеспечению; статистическим методом автор пользовался в процессе обоснования опасности данной формы преступности; системно-структурный метод был выбран для классификации видов преступлений, направленных против компьютерной информации; логико-юридический метод использован при разработке предложений относительно изменений в действующее законодательство с целью совершенствования нормативно-правовой базы, которая формирует правовой механизм противодействия данной форме преступности.

Теоретическую основу исследования составили труды по философии, управлению в социальных и экономических системах, теории информации и теории безопасности, науке уголовного права, криминологии и социологии, которые раскрывают проблемы общей безопасности, информационной безопасности, а также вопросы, связанные с безопасностью компьютерной информации.

К проблемам философского осмысления безопасности в различных сферах общественной жизни обращались Т.Г. Антропова, Б.М. Дошаев, А.К. Есаян, Т.А. Мешкова, Ю.Н. Рагозин, В.К. Сенчагов, которые своими работами заложили основы понятия «безопасность», в том числе и в информационной сфере.

К вопросам правового обеспечения информационной безопасности в своих научных трудах обращались: П.Г. Андреев, А.В. Бубнов, Л.А. Букалерова, Д.С. Будаковский, Н.И. Бусленко, А.Г. Волеводз, В.Б. Вехов, В.И. Гладких,

М.Ю. Дворецкий, А.М. Доронин, К.Н. Евдокимов, А.А. Задков, М.А. Ефремова, Е.А. Зверева, У.В. Зинина, И.Г. Иванова, А.Ж. Кабанова, В.В. Крылов, Д.А. Калмыков, А.Ю. Карманов, В.С. Карпов, В.А. Копылов, А.Н. Копырюлин, Е.В. Красненкова, П.У. Кузнецов, Т.А. Лопатина, Е.В. Михайленко, Т.А. Полякова, О.М. Сафонов, А.А. Стрельцов, М.В. Талан, О.М. Цыденова, Н.И. Шумилов, Д.А. Ястребов и др.

Указанные ученые создали солидную теоретическую базу, обеспечивающую практические основы уголовно-правовой защиты компьютерной информации. В то же время, динамичный характер современной информационной среды, возникновение новых вызовов и угроз в данной сфере требует продолжения научно-теоретической разработки данной проблемы.

Нормативная база исследования включает положения Конституции Российской Федерации, международные правовые акты и рекомендации, принятые международными организациями в части обеспечения безопасности компьютерной информации, нормы уголовного, уголовно-процессуального, административного, информационного и иного законодательства Российской Федерации, регулирующие отношения, обеспечивающие национальную, информационную безопасность. В работе использованы нормативные правовые акты федеральных органов государственной власти РФ (указы Президента РФ, постановления Правительства РФ, приказы и иные подзаконные акты министерств и ведомств РФ). Кроме того, использованы нормы уголовного законодательства ряда зарубежных государств (Республики Армения, Республики Беларусь, Республики Казахстан, Соединенных Штатов Америки).

Эмпирическую основу диссертации составили статистические данные, касающиеся вопросов уголовно-правовой охраны безопасности компьютерной информации, размещенные на официальных сайтах МВД России, Генеральной Прокуратуры Российской Федерации, Министерства юстиции Российской Федерации, в том числе, размещенные в сети Интернет.

Положения и выводы диссертанта базируются на обобщении материалов 270 уголовных дел, рассмотренных судами в период с 2004 по 2014 гг. в 36

субъектах Российской Федерации.

При обосновании выводов, предложений и положений, выносимых на защиту, использованы материалы аналитических обобщений Следственного департамента МВД России, информационные материалы в СМИ, а также результаты научных исследований других авторов.

Научная новизна диссертационного исследования определяется получением совокупности новых знаний, выраженных в комплексе научно-теоретических (доктринальных), законотворческих и прикладных выводов, положений и предложений, составляющих единое цельное и непротиворечивое учение (частную теорию) обеспечения безопасности компьютерной информации с помощью уголовно-правовых средств. В частности, новизна диссертационного исследования заключается в том, что автором на основе проведенного комплексного анализа современных научно-практических проблем, связанных с уголовно-правовым обеспечением безопасности компьютерной информации, определен круг проблемных вопросов в теории уголовного права, в уголовном законодательстве и в правоприменительной практике, предложены способы их решения, раскрыты сущность и содержание методологического и законодательного обеспечения безопасности компьютерной информации, международно-правовые и национальные (конституционно-правовые и уголовно-правовые) основы борьбы с преступлениями против компьютерной информации, а также рассмотрены все составы преступлений против компьютерной информации, изучена практика их применения, сформулированы выводы и внесены конкретные предложения по совершенствованию уголовно-правовых норм, обеспечивающих охрану компьютерной информации от преступных посягательств.

Новизна диссертации определяется полученными выводами и результатами исследования и положениями, выносимыми на защиту.

Положения, выносимые на защиту.

1. Комплекс научно-теоретических положений (частная теория) методологического и законодательного обеспечения безопасности

компьютерной информации с помощью уголовно-правовых средств, включающее в себя доктринальные позиции автора:

1) о сущности и содержании методологического и законодательного обеспечения безопасности компьютерной информации;

2) о международно-правовых и национальных (конституционно-правовых и уголовно-правовых) основах борьбы с преступлениями против компьютерной информации;

3) о понятии преступлений против компьютерной информации, их предмете и классификации;

4) о характеристике элементов составов преступлений против компьютерной информации и их отграничении от смежных составов преступлений;

5) о путях и способах совершенствования уголовно-правовой защиты компьютерной информации в Российской Федерации;

6) о действии уголовного закона во времени и в пространстве применительно к преступлениям против компьютерной информации;

7) о содержании изменений и дополнений в действующее уголовное законодательство;

8) о целесообразности обобщения судебной практики и содержании разъяснений высшей судебной инстанции – Пленума Верховного Суда Российской Федерации по делам о преступлениях против компьютерной информации.

2. Интенсивное развитие информационного общества обязывает государство повышать уровень информационной безопасности общества и особое внимание обращать на борьбу с компьютерными преступлениями. Вместе с тем, уголовная политика в сфере борьбы с компьютерными преступлениями должна содержать не только правовые, но и экономические, социальные, организационные и другие меры. Новым трендом политики государственного принуждения должно стать повышение правовой и общей культуры граждан, их правосознания, а также эффективности деятельности

государственных органов по профилактике компьютерных преступлений.

3. Вопрос обеспечения информационной безопасности как одной из важных составляющих национальной безопасности государства особенно остро встает в контексте появления транснациональной (трансграничной) компьютерной преступности и кибертерроризма. Учитывая, что информационное пространство все больше становится ареной противостояния, критически важной становится проблема международно-правового регулирования правоотношений в телекоммуникационных сетях. Поэтому заслуживает поддержки позиция Российской Федерации, придающей важное значение международной информационной безопасности как одному из ключевых элементов системы коллективной безопасности, и выступающей за принятие под эгидой Организации Объединенных Наций Конвенции об обеспечении международной информационной безопасности как международно-правовой основы координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий.

4. Авторские определения:

– *преступления против компьютерной информации* – как умышленного общественно опасного деяния (действия или бездействия), причиняющего вред общественным отношениям, регламентирующим безопасное создание, хранение, использование или передачу компьютерной информации;

– *видового объекта преступления* главы 28 УК РФ как общественных отношений, обеспечивающих безопасность компьютерной информации;

– *предмета преступлений против компьютерной информации* как сведений (сообщений, данных), представленных в виде электрических сигналов, которые могут храниться, использоваться или передаваться с применением средств компьютерной техники. К предмету преступлений против компьютерной информации не могут быть отнесены средства компьютерной техники и средства хранения компьютерной информации.

5. Вывод о необходимости закрепления нового наименования главы 28 УК

РФ в виде следующей формулировки «Преступления против компьютерной информации». Новое название направлено на поддержание системности УК РФ и соответствует традиционному подходу российского уголовного права к объекту посягательства как сфере социальных отношений.

6. Авторская позиция о применении уголовного закона в зависимости от места нахождения преступника в момент совершения им посягательства на компьютерную информацию. В случае наступления общественно опасных последствий на территории третьих государств вопрос о применимом уголовном законе должен решаться каждый раз индивидуально по соглашению государств с учетом соблюдения общепризнанного правового принципа non bis in idem.

7. Научно-теоретическая (доктринальная) модель законодательной регламентации преступлений против компьютерной информации, включающая в себя новые редакции статей 272 и 273 УК РФ.

«**Статья 272. Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а равно ознакомление с содержанием компьютерной информацией, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до

двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору либо лицом с использованием своего служебного положения, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они совершены организованной группой либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.».

«**Статья 273. Незаконное хранение, использование, распространение и приобретение вредоносных компьютерных программ**

1. Незаконное создание, хранение, использование, распространение и приобретение компьютерной программы либо иной компьютерной информации, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы

на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они совершены организованной группой либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.».

8. Вывод автора о необходимости обобщения судебной практики и авторский проект Постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях против компьютерной информации» (Приложение № 2).

Теоретическая и практическая значимость исследования. Сформулированные автором общетеоретические положения и выводы вносят существенный вклад в юридическую науку, а именно в теорию уголовного права. Они представляют несомненную ценность для смежных отраслей юридической науки, а именно, для криминологии – в части предупреждения преступлений против компьютерной информации и теории уголовно-исполнительного права – в части исполнения наказания в отношении

осужденных за данные виды преступлений. Кроме того, результаты исследования обладают потенциалом для дальнейших научных разработок, касающихся проблем уголовной ответственности за преступления, направленные против компьютерной информации.

Выводы, рекомендации и предложения диссертационной работы могут быть использованы при решении прикладных проблем, в частности в процессе совершенствования уголовного законодательства, регулирующего безопасность компьютерной информации, для обеспечения правильной уголовно-правовой классификации данных преступлений, для разработки рекомендаций работникам правоохранительных и судебных органов по поводу правомерности применения норм УК РФ, направленных на обеспечение безопасности в данной сфере общественных отношений.

Теоретические положения и выводы, предложения по совершенствованию законодательства и практические рекомендации диссертационного исследования могут быть использованы в правотворческой и правоприменительной деятельности правоохранительных и судебных органов, в процессе преподавания дисциплинам «Уголовное право», «Криминология», «Уголовно-исполнительное право» «Конституционное право», «Информационное право» в профессиональных образовательных организациях и в образовательных организациях высшего образования Российской Федерации, а также при подготовке научных монографий, методических материалов, учебных и учебно-методических пособий по данной тематике.

Степень достоверности полученных результатов. Степень достоверности результатов диссертационного исследования обусловлена методологией исследования, комплексным подходом к изучению уголовно-правового регулирования безопасности компьютерной информации в Российской Федерации.

Обоснованность и достоверность результатов проведенного исследования обеспечиваются также репрезентативностью собранного и проанализированного эмпирического материала, на котором основываются

разработанные в диссертации научные положения. В диссертации широко представлены результаты эмпирических исследований других авторов, на основе которых делались закономерные обобщения, подтверждались выводы и разработанные рекомендации.

В качестве эмпирической базы исследования диссертантом были использованы нормы международного права, законодательство РФ и иностранных государств, статистические данные ГИАЦ МВД России, Минкомсвязи России, архивные материалы судов за 2004-2010 гг. в количестве 270 уголовных дел, 23 материала об отказе в возбуждении уголовного дела, постановления Пленума Верховного Суда РФ, обобщения судебной практики, проведенные судами ряда субъектов РФ и их аналитические записки.

Апробация результатов исследования и внедрение их в практику. Диссертационное исследование является результатом десятилетней научно-педагогической деятельности соискателя. Результаты работы, основанные на них выводы, положения и рекомендации, обсуждались на кафедре уголовного права и криминологии Юридического факультета МГУ имени М.В. Ломоносова, докладывались на Ученом совете Юридического факультета МГУ имени М.В. Ломоносова 21 февраля 2014 года. По проблемам диссертации опубликована 31 научная работа, в частности 24 статьи в научных изданиях, рецензируемых Высшей аттестационной комиссией при Минобрнауки России, общим объемом 15.5 п. л., а также 1 монография объемом 13 п. л.

Материалы диссертационного исследования внедрены в практическую деятельность Комитета по гражданскому, уголовному, арбитражному и процессуальному законодательству Государственной Думы Федерального Собрания Российской Федерации и публичного акционерного общества «Ростелеком». Результаты исследования были внедрены в учебный процесс Юридического факультета МГУ имени М.В. Ломоносова.

Структура и объем диссертации. Структура представленной работы соответствует логике проведенного исследования. Диссертационное исследование состоит из введения, пяти глав, семнадцати параграфов,

заключения, списка использованной литературы, а также приложений, в том числе проекта Постановления Пленума Верховного Суда РФ «О судебной практике по делам о преступлениях против компьютерной информации».

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во **введении** обосновывается актуальность темы, формулируется цель и задачи исследования, его объект и предмет, характеризуется методологическая, нормативная, теоретическая и эмпирическая основы диссертации, определяется ее научная новизна и положения, выносимые на защиту, доказывается их теоретическая ценность и практическая значимость, содержатся сведения об апробации основных выводов и предложений.

Глава 1 «Методологическое обеспечение регулирования безопасности компьютерной информации в уголовно-правовом аспекте» состоит из трех параграфов.

В первом параграфе «Теоретические основы уголовно-правового обеспечения безопасности компьютерной информации» констатируется, что процессы информатизации и компьютеризации в начале XXI в. охватили все стороны общественной жизни, что во многом определяет направление и содержание текущих социальных трансформаций. Подчиняясь законам диалектики, эти трансформации нельзя считать однозначными, вместе с возможностью удовлетворения информационных потребностей человека возникает и целый комплекс негативных социальных тенденций, в частности речь идет о развитии различных видов противоправного использования современных компьютерных технологий в преступных целях.

Современная Россия в полной мере включена в процессы информатизации общества и формирования единого мирового информационного рынка. Информационный фактор играет значительную роль в государственно-созидательном процессе, в представлении и отстаивании интересов государства. Особое место в этом спектре общественных отношений занимают проблемы правового обеспечения информационной безопасности.

Среди мотивов совершения компьютерных преступлений доминирует желание незаконного получения материальной выгоды; количество совершения преступлений с иным мотивом, например, хулиганским, – незначительно. Если в 2013 г. данный мотив присутствовал в 30% преступлений в информационной сфере, то 2014 г. их доля составила уже 41%. В данной преступной деятельности широко используются различные вредоносные программы, которое ориентированы на хищение средств с банковских счетов, на удаленное получение контроля над компьютерными и мобильными устройствами.

Данная преступная деятельность наносит значительный урон, становится проблемой национального масштаба, поскольку, например, объем денежных средств, похищенных преступниками с платежных карт россиян, составил в 2013-2014 гг. порядка 680 млн. долл. США. При этом все чаще преступники посягают на безопасность компьютерной информации, на финансовые ресурсы организаций финансового сектора и государственного сектора экономики.

Необходимо осознавать, что наука уголовного права представляет собой элемент общеправовой теоретической системы, который обеспечивает на практике научный подход в разработке уголовной политики. Соответственно теоретическое обоснование проблемы безопасности компьютерной информации имеет прямое отношение к решению проблемы противодействия компьютерной преступности, разработке уголовной политики, направленной на обеспечение безопасности компьютерной информации.

Данную проблему актуализирует и необходимость осмысления феномена компьютерной преступности как принципиально новой формы противоправной уголовно-наказуемой деятельности, для которой характерны использование новейших информационных технологий, дающих возможность совершать преступления отдаленно, при отсутствии непосредственного контакта между жертвой и преступником, а также большие возможности сокрытия преступной деятельности и их анонимизации и наличия существенного временного разрыва между началом активных действий и наступлением последствий.

В числе особенностей компьютерных преступлений отмечается их транснациональность (межграничность), значительно усложняющая установление места совершения преступлений, их раскрытие, расследование и

профилактику. При этом данная форма преступности формирует материальную базу для иных форм преступности, в том числе и для совершения насильственных видов преступлений, в частности террористических актов.

Рассматривая проблемы, касающиеся безопасного обращения компьютерной информации, автор обращается к базовому понятию «безопасность», которое, несмотря на свою кажущуюся очевидность, несет в себе глубокий смысл, о чем свидетельствует внимание выдающихся мыслителей к данной дефиниции.

Проведенный философско-правовой анализ показал, что вопросы безопасности на всех этапах развития человеческой цивилизации были и остаются актуальными. При этом безопасность формируется в двух параллельных плоскостях: в плоскости личной безопасности каждого отдельно взятого субъекта, а также в плоскости безопасности государства, которое со своей стороны должно обеспечить безопасность личности, а личность, имея гарантированные права и свободы, в своей деятельности соблюдает требования правовых норм, принимаемых государством.

Диссертант характеризует безопасность как состояние защищенности личности, общества и государства от различных угроз, которое достигается посредством нормативно-правового регулирования той или иной сферы деятельности личности, общества и государства.

Что касается проблем, связанных с безопасным обращением компьютерной информации, то данная сфера безопасности самым тесным образом связана с природой и содержанием информационного обмена, оборота информации.

В диссертации констатируется, что отсутствие единого понимания сущности информации как ключевой составляющей информационного общества и мирового информационного пространства следует рассматривать как системную проблему.

Информационная безопасность достигается путем реализации соответствующего комплекса мероприятий, которые могут быть методами, процедурами, организационными структурами и функциями программного

обеспечения. Указанные мероприятия должны обеспечить достижение целей информационной безопасности организации.

Согласно же действующему законодательству, защита информации представляет собой принятие правовых, организационных и технических мер, направленных на: обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа; реализацию права на доступ к информации (ч. 1 ст. 16 Федерального закона «Об информации, информационных технологиях и о защите информации»).

Достижение данных целей возможно путем правового регулирования, которое должно обеспечить целенаправленное воздействие на общественные отношения в информационном пространстве с помощью правовых (юридических) средств.

Сами по себе информационные отношения возникают и развиваются во всех видах социальной деятельности: в сфере государственного управления, в конституционных, гражданско-правовых, административных, уголовно-правовых отношениях. Столь широкий спектр общественных отношений, возникающих в процессе обращения информации, требует того, чтобы вопросы информационной безопасности решались путем использования комплексного механизма правовой защиты на основе применения не только норм собственно информационного права, но и с использованием норм конституционного, административного, гражданского, хозяйственного, банковского и уголовного права.

Таким образом, определенные виды информационных отношений в обществе регулируются правовыми нормами, которые, прежде всего, регламентируют параметры информационных процессов в той или иной сфере нормативно-правового регулирования. Безусловно, оборот различных видов информации (например, частной, коммерческой информации, которая составляет военную, государственную тайну), регулируется специальными правовыми нормами, которые соответствуют ее специфике. В зависимости от

вида информации законодательство предусматривает наличие или отсутствие тех или иных ограничений или запретов. Соответственно в теории выделяют две основные группы информации: открытая (свободно распространяемая в информационной сфере), и информация ограниченного доступа (распространение которой возможно лишь на условиях конфиденциальности или секретности).

В качестве основы для классификации информационных отношений предлагается такой критерий, как метод правового регулирования, касающийся оборота (обращения) информации. В соответствии с диспозитивным методом условия обращения информации, порядок ее использования, распространения, передачи прав третьим лицам определяются либо владельцем этой информации лично, либо на основе договора с заинтересованными лицами. Императивный метод характеризуется наличием четких законодательных предписаний, отмена и изменение которых по согласию сторон невозможна.

В ряде случаев, в зависимости от социальной значимости информации, ее охрана обеспечивается нормами уголовного права, хотя, при этом, следует указать на тот факт, что непосредственно понятие «информационая безопасность» в УК РФ не используется. По мнению автора, данное обстоятельство следует рассматривать как пробел, в связи с чем в работе делается вывод о необходимости закрепления нового наименования главы 28 УК РФ «Преступления против компьютерной информации». Новое название направлено на обеспечение системности уголовного закона и соответствует традиционному подходу российского уголовного права к объекту посягательства как сфере социальных отношений.

Что касается оснований уголовной ответственности за преступления в информационной сфере, то они, по сути, являются традиционными для любого уголовно-наказуемого деяния. Речь идет о противоправности, которая выражается в нарушении определенных правовых норм, обеспечивающих информационную безопасность; об общественной опасности; о наказуемости, особенностью которой является то, что за то или иное деяние предусмотрена уголовная ответственность; о виновности, которая выражается в форме действия или бездействия; о причинной связи между противоправным

действием и наступившими в результате его общественно опасными последствиями.

Говоря о конкретизации понятия «безопасность компьютерной информации» в уголовно-правовом смысле, диссертант подчеркивает, что оно, являясь объектом уголовно-правовой защиты, представляет собой состояние защищенности информации, которая может являться предметом информационного обмена, храниться на жестком диске компьютера, в компьютерных сетях, на иных информационных носителях. Таким образом, безопасность компьютерной информации – это состояние ее защищенности от угроз неправомерного доступа и вредоносных компьютерных программ.

Непосредственно состояние безопасного обращения компьютерной информации достигается, в том числе, и уголовно-правовыми мерами, определяющими преступность и наказуемость деяний, связанных с посягательствами против компьютерной информации. Предметом преступлений против компьютерной информации являются сведения (сообщения, данные), представленные в виде электрических сигналов, которые могут храниться, использоваться или передаваться с применением средств компьютерной техники. К предмету преступлений против компьютерной информации не могут быть отнесены средства компьютерной техники и средства хранения компьютерной информации.

Безопасность компьютерной информации включает в себя две составляющие: техническую, требующую для достижения состояния безопасности использования средств технической защиты, и юридическую, когда защита информации осуществляется посредством использования средств правового регулирования. Если техническая составляющая способна обеспечить безопасное обращение компьютерной информации, хранящейся на любом носителе, в том числе на жестком диске компьютера, на мобильном телефоне, в локальной либо глобальной сети, на иных носителях информации, то юридический смысл зашиты информации подразумевает ее защиту нормами конституционного, гражданского, информационного, административного и уголовного права.

Уголовная ответственность за преступления против информационной безопаности определяется статьями УК РФ, которые расположены в различных разделах и главах. Из общего перечня информационных отношений, которые подлежат уголовно-правовой охране, особо выделены отношения, возникающие в связи с уголовно наказуемыми посягательствами в сфере компьютерной информации (гл. 28 УК РФ). Речь идет о неправомерном доступе к компьютерной информации (ст. 272 УК РФ), о создании, использовании и распространении вредоносных компьютерных программ (ст. 273 УК РФ), о нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ).

Вместе с тем, фактически, «информационная» составляющая присутствует и в ряде иных составов преступлений, которые хотя напрямую не посягают на информационную безопасность, не ставят целью хищение, уничтожение, модификацию информации, но, тем не менее, имеют ярко выраженное негативное информационное воздействие. Таким образом, несмотря на отсутствие в нормах УК РФ такого понятия, как информационная безопасность, фактически исследуемое понятие входит в целый ряд его норм и на семантическом уровне присутствует в диспозициях статей в виде специфических терминов, таких как «разглашение», «распространение», «незаконное изготовление», «незаконный оборот».

Несмотря на то, что информационная безопасность традиционно ассоциируется, главным образом, с компьютерными технологиями и совершаемыми в этой сфере правонарушениями, значительное количество статей УК РФ направлено на защиту иных отношений, в которых использование компьютерной техники и информационных технологий не предполагается либо таковое использование не является определяющим.

Речь идет об обеспечении сохранности различных видов тайн (личной, государственной), обеспечении неприкосновенности частной жизни, а также чести и достоинства человека и гражданина, об обеспечении права на доступ к информации, права на комфортную информационную среду, не посягающую на мораль, нравственность, психологический комфорт личности.

Следующий параграф посвящен анализу понятийного аппарата, применяемого при исследовании преступлений в сфере компьютерной информации. Обращается внимание на тот факт, что он представляет собой сложную, динамичную систему, которая формировалась на протяжении столетий, и данное развитие интенсивно происходит в настоящее время. В частности, динамический характер лексики уголовного права самым тесным образом связан с динамическими процессами, происходящими в информационной сфере, с появлением новых форм преступности в сфере обращения информации.

Анализ терминологического поля безопасного обращения компьютерной информации в первую очередь требует уточнения содержания термина самого «компьютерная информация», который самым тесным образом связан с понятием «компьютерные данные».

В Конвенции о киберпреступности компьютерные данные определены как любое представление фактов, информации или понятий в форме, подходящей для обработки в компьютерной системе, включая программы, способные заставить компьютерную систему выполнять ту или иную функцию».

На Десятом Конгрессе ООН по предупреждению преступности и обращению с правонарушителями в Справочном документе для семинара-практикума по преступлениям, связанным с использованием компьютерной сети, термин «данные» определялся как факты, инструкции или концепции, излагаемые обычным образом, в форме, поддающейся пониманию человеком или автоматизированной обработке.

Федеральным законом от 07.12.2011 № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации» впервые введено понятие компьютерной информации, необходимость чего подчеркивалось в доктрине уголовного права. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Данное определение в диссертации оценивается критически, указываются его технико-юридические недостатки.

Автор констатирует, что несмотря на отсутствие юридического определения понятий «киберпространства», «киберпреступления» они стали общеупотребительными в доктрине уголовного права. Зачастую они используются как синонимы терминов «информационное пространство», «компьютерное преступление». В уголовном праве это особенно важно, так как правильная квалификация деяния должна основываться на четком понимании объекта и предмета преступления и оценке его общественной опасности. Вместе с тем, обосновывается, что с точки зрения уголовно-правовой семантики целесообразно отойти от «кибер»-терминологии и перейти к таким понятиям, как «информация», «информационная сфера», «информационная система», «компьютерная преступность» и т.д.

Представляется важным также введение родового понятия, касающегося уголовно ненаказуемых неправомерных деяний в информационной сфере – понятия «компьютерное правонарушение», что обеспечит дифференциацию уголовной ответственности, индивидуализацию наказания. Данное противоправное действие может быть определено как виновное деяние, которое осуществляется с использованием технологий преобразования (создания, хранения, обмена, обработки и уничтожения) информации, представленной в виде цифровых данных, и влечет за собой юридическую ответственность. Компьютерное правонарушение имеет все общие признаки правонарушений, выделяемых в теории права, и отличается лишь факультативной частью юридического состава, в котором информационное пространство выступает как средство совершения правонарушения.

Сфера обмена и обработки компьютерной информации играет все большую роль в процессах развития российского общества, а криминальные проявления в этой сфере приобретают угрожающие масштабы. Это предопределяет необходимость охвата ее регулятивными и охранительными функциями права, а также повышает внимание к информационной безопасности как к отдельной составляющей национальной безопасности России. В таких условиях важным является системный подход к формированию понятийно-терминологического аппарата безопасного обращения компьютерной информация, который обеспечит ее адекватное содержательное

наполнение, соответствие требованиям, предъявляемым к правовой терминологии, а также гармонизацию с традициями русского уголовного права и терминологией действующего уголовного законодательства.

В следующем параграфе анализируются методические основы познания уголовно-правовой охраны компьютерной информации. Необходимыми условиями развития информационного общества являются создание действенного механизма правовой защиты личности, общества и государства, как субъектов информационной деятельности; выработка мер, способствующих снижению уровня компьютерной преступности; установление эффективных карательных мер в отношении лиц, совершивших компьютерные преступления.

Решение данных вопросов, в теоретико-прикладном аспекте, представляется затруднительным без надлежащего методологического и методического обеспечения процесса исследования процесса уголовно-правового регулирования безопасного обращения компьютерной информации.

Анализ научных позиций относительно содержания диалектики в правовых исследованиях позволил автору сформулировать вывод о трехчленной структуре методологии науки уголовного права, включающей философский (фундаментальный), общенаучный и конкретно-научный уровень.

Рассматривая проблемы методологии в связи с проблемами познания на уровне терминологии, обращается внимание на различие понятий «подход» и «метод». Первый указывает на наличие альтернативы и исключает единственно правильную методологию. В рамках одного подхода может использоваться целая совокупность методов. К подходам часто относят все возможные познавательные средства (аксиологический, антропологический, экономический, тендерный, гуманистический, социологический и т.д.).

Подходы возможно структурировать на те, которые сосредотачиваются в «верхней части» методологии – теоретико-мировоззренческом блоке, и те, которые находятся в нижнем – инструментальном блоке методологии.

При этом следует подчеркнуть, что методика познания и анализа процесса уголовно-правового регулирования безопасности компьютерной информации должна базироваться на методологических основаниях информационного и уголовного права. В отличие от других отраслей права, в том числе и

уголовного, где четко определены предмет и метод, информационное право находится в стадии своего становления и теоретического обоснования. В зчастности, в Российской Федерации, информационное право рассматривается как комплексная отрасль права. Объединяющая очень большой комплекс отношений, связанных с формированием информационных ресурсов, созданием и использованием технологий их обработки и применения, обеспечением их коммуникации в системах и сетях, эта совокупность отношений на полном основании должна быть выделена в самостоятельную отрасль права – информационное право. Уголовно-правовая охрана безопасного обращения компьютерной информации предполагает первичное нормативно-правовое урегулирование общественных отношений нормами информационного права. Именно наличие уголовно-правовых норм обеспечивает информационное право реальной возможностью защищать информационные отношения от преступных посягательств, обеспечивая законные интересов всех участников информационных отношений.

В диссертации обозначены перспективы использования при исследовании такого объекта уголовно-правовой охраны, как правопорядок в сфере безопасного обращения компьютерной информации, его сторон и механизма причинения ему вреда, синергетического метода, метода системно-структурного анализа, герменевтического метода.

Особая роль отводится системному подходу, предполагающему рассмотрение частей в единстве с целым, с учетом связей и отношений системы со средой, в которой она находится. Именно системный подход может быть использован в исследовании связей уголовного законодательства и положений иных правовых актов об охране информации (или, что более точно соответствует предметной специфике последнего – информационного права), административного законодательства, некоторых конституционных положений. На данном основании, в частности, могут быть выявлены признаки, позволяющие отграничивать преступные посягательства на правопорядок в сфере безопасного обращения компьютерной информации от неуголовных девиаций в этой сфере. Также вышеупомянутые признаки позволяют очертить пределы уголовно-правовой защиты указанного объекта, обнаружить в ней

пробелы – сегменты в системе отношений в сфере информационной деятельности, которые не нуждаются в уголовно-правовой защите.

В целом же, при исследовании проблем, касающихся уголовно-правовой защиты безопасного обращения компьютерной информации, применим комбинированный подход, основанный на использовании широкого спектра методов, входящих в инструментарий наук уголовного и информационного права, на основе системного, межотраслевого анализа уголовно-правовых явлений, воздействующих на процессы безопасного обращения компьютерной информации.

Глава 2 «Правовые основы противодействия преступлениям против компьютерной информации» включает в себя три параграфа. В первом из них исследуются международно-правовые основы противодействия преступлениям против компьютерной информации.

В настоящее время нормативно-правовое обеспечение деятельности, регулирующей процесс безопасного обращения компьютерной информации, требует новых подходов, которые должны учитывать интересы всех стран.

Право на свободу получения информации обеспечено международным правом, но, в тоже время, оно не является абсолютным, поскольку всегда ограничено правом государства и личности ограничивать доступ к информации, которая является государственной тайной, личной информацией, не подлежащей разглашению. Фактически речь должна идти о создании нормативно-правовых основ обеспечения безопасного обращения компьютерной информации на международном уровне, которые, в первую очередь, касаются проблем информационной безопасности.

Базовые принципы международной информационной безопасности определяют роль и права, обязательства и ответственность государств в информационном пространстве, конкретные задачи, решение которых было бы направлено на ограничения угроз в сфере информационной безопасности, а также определяют роль ООН в контексте общих усилий в этой сфере.

В материалах Десятого Конгресса ООН 2000 г. по предупреждению преступности и обращению с правонарушителями выделены две категории преступлений:

1) компьютерные преступления (киберпреступления в терминологии ООН) в узком смысле («компьютерные» преступления) – любое противоправное деяние, осуществляемое путем электронных операций, целью которого является преодоление защиты компьютерных систем и обрабатываемых ими данных;

2) компьютерные преступления в широком смысле (преступления, связанные с использованием компьютеров) – любое противоправное деяние, которое совершается в связи с использованием компьютерной системы или сети, включая такие преступления, как незаконное хранение, предложение или распространение информации через компьютерные системы или сети.

Кроме того, в соответствии с рекомендациями резолюции 55/28, был подготовлен проект документа (A/56/164/Add.1) «Общая оценка проблем информационной безопасности. Угрозы международной информационной безопасности», в котором выделены и описаны одиннадцать основных факторов, создающих опасность основным интересам личности, общества и государства в информационном пространстве, то есть являются наибольшими угрозами информационной безопасности.

К таким факторам относятся: разработка и использование средств несанкционированного вмешательства в работу информационных компьютерных технологий, неправомерное использование и нанесение ущерба информационным ресурсам другого государства; целенаправленное информационное воздействие на критические инфраструктуры и населения другого государства; действия, направленные на доминирование в информационном пространстве, поощрение терроризма и ведения информационных войн.

Генеральная Ассамблея ООН 22.11.2002 приняла резолюцию по информационной безопасности (A/RES/57/53), которая развивает положения предыдущих резолюций и указывает на недопустимость использования информационно-телекоммуникационных технологий и средств с целью оказания негативного воздействия на инфраструктуру государств. Резолюция определяет также направления деятельности ООН, которая должна быть сконцентрирована на следующих основных моментах, в частности, на

согласование понятийного аппарата в сфере информационной безопасности, что по нашему мнению является ключевым в данном документе.

К сожалению, большинство положений данного документа (согласование понятийного аппарата в сфере информационной безопасности, рассмотрение возможных путей международного взаимодействия правоохранительных органов по предотвращению и пресечению правонарушений в информационном пространстве, в частности, по выявлению источников информационной агрессии) остались нереализованными до настоящего времени.

Последние Резолюции Генеральной Ассамблеи ООН, посвященные вопросам борьбы с преступлениями в сфере информационных технологий, призывают к серьезному отношению и рассмотрению на международном уровне существующих и потенциальных угроз в сфере информационной безопасности, а также принятию возможных мер по ограничению таких угроз. Так, например, Резолюция от 02.12.2009 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» в целях поддержания целостности гражданской и военной инфраструктур государств – членов предлагает поддержать международное сотрудничество на многостороннем уровне, в частности, осуществлять взаимное информирование в таких вопросах, как: a) оценка проблем информационной безопасности; b) укрепление информационной безопасности и содействия международному сотрудничеству в этой области; c) содержание международных концепций, направленных на укрепление безопасности глобальных информационных и телекоммуникационных систем; d) меры, необходимые к принятию для укрепления информационной безопасности на глобальном уровне.

В контексте рассмотрения международно-правовых актов, посвященных вопросам информационной безопасности, нельзя не признать, что действенность, результативность и эффективность информационных отношений напрямую зависят от того, насколько они обеспечиваются средствами правовой охраны, реализация чего не может быть выполнена без формирования научно обоснованной системы правового обеспечения информационной среды.

Наиболее важным международным документом является Конвенция Совета Европы о киберпреступности 2001 г., целью которой, как указано в преамбуле, является поддержание «общей уголовной политики, нацеленной на защиту общества от киберпреступлений, через принятие соответствующих законодательных актов и укрепление международного сотрудничества». Конвенция не только рекомендует государствам-участникам закрепить на уровне национального законодательства важнейшие составы компьютерных преступлений, но и предписывает предпринимать конкретные организационные меры по борьбе с ними. Часть правовых норм Конвенции посвящена регламентации механизма международного сотрудничества в проведении расследований компьютерных преступлений, в уголовном преследовании.

По мнению диссертанта, в современных условиях международно-правовая база, касающаяся безопасного обращения компьютерной информации, нуждается в дальнейшем совершенствовании. Необходимо на уровне ООН принять единую Конвенцию, касающуюся вопросов безопасного обращения компьютерной информации и противодействия компьютерным преступлениям, которая пришла бы на смену устаревшим международно-правовым документам и учла последние тенденции, связанные с развитием данной формы преступности.

В 2012 г. аппаратом Совета Безопасности Российской Федерации, МИД России и Институтом проблем информационной безопасности МГУ был представлен проект конвенции ООН «Об обеспечении международной информационной безопасности». Подготовка такого документа была связана с актуальной необходимостью принятия свода специальных международных правил поведения в глобальном киберпространстве. Однако на международном уровне этот проект не получил широкой поддержки.

Подводя итог анализу международно-правового регулирования компьютерных преступлений, следует отметить, что большинство документов, таких как рекомендации Совета Европы, различные документы ООН, носят рекомендательный характер и не обязательны для применения. На настоящий момент существует обязательный для государств-участников документ – Конвенция о киберпреступности 2001 г., которая играет главную роль в

международно-правовом регулировании компьютерной преступности. Однако Конвенция не ратифицирована Россией, которая фактически не принимает участие ни в одном универсальном международном договоре, регулирующем вопросы компьютерных преступлений.

Единственным обязательным для России международно-правовым документом в данной области является Соглашение о сотрудничестве на уровне СНГ. В то же время именно Россия находится в настоящее время в авангарде решения проблемы разработки нормативно-правовых основ обеспечения безопасного обращения компьютерной информации на международном уровне, подтверждением чего явился проект концепции Конвенции об обеспечении международной информационной безопасности.

Рассматривая в следующем параграфе конституционные основы уголовно-правового противодействия преступлениям против компьютерной информации, автор акцентирует внимание на том, что Конституция Российской Федерации является одним из важнейших источников права, гарантируя право на информацию, обеспечивая ее безопасное обращение, формируя основы правового регулирования безопасного обращения. Непосредственно реализация данных прав опирается соответствующий конституционно-правовой механизм.

Нормы Конституции РФ соответствуют фундаментальным основам международного права, регулирующего безопасный оборот информации, а также права человека и гражданина в данной сфере общественных отношений.

Главным международно-правовым стандартом в области прав человека является комплексный акт, разработанный в рамках ООН и известный как Хартия о правах человека. Первым фундаментальным международно-правовым актом в рамках Хартии о правах человека является Всеобщая декларация прав человека, принятая Генеральной Ассамблеей ООН 10.12.1948. Эта декларация содержит целый комплекс юридических гарантий, которые определяют содержание и сущность информационной безопасности личности.

Конституционное право ориентируется на регулирование информационно-правовых отношений, которые имеют фундаментальное значение для государства, общества, человека и гражданина, в частности право на информацию, право каждого свободно искать, получать, передавать,

производить и распространять информацию любым законным способом (ч. 4 ст. 29 Конституции РФ). В свою очередь, на практике реализация информационно-правовых отношений происходит в таких формах, как соблюдение запретов, исполнение обязанностей, использование прав и свобод, которые образуют механизм реализации прав и свобод человека и гражданина.

Рассматривая данную сферу общественных отношений, диссертант признает, что сегодня фактически отсутствует понимание сущности механизма реализации прав и свобод человека в сфере информационных отношений, и этот вопрос требует отдельного подробного исследования.

Под конституционно-правовым механизмом обеспечения безопасного обращения информации в Российской Федерации предлагается понимать систему конституционно-правовых норм и правовых гарантий, направленных на защиту интересов государства и общества, обеспечение прав и свобод человека и гражданина в информационной сфере, определяющих меру ответственности за нарушение данного права.

Особое значение информационной деятельности, использования информационных технологий, а также компьютерной техники во всех сферах жизнедеятельности государства, общества, человека и гражданина является тем фактором, который определяет регулирование данной деятельности нормами Конституции РФ. В этом смысле главной особенностью правового регулирования информационных отношений является то, что его основу, его юридический базис, составляют информационные права и свободы, среди которых главное место занимает право каждого гражданина свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п. 4 ст. 29). Фактически данная конституционная норма гарантирует каждому право на свободный доступ к информации, которое является правовой категорией, требующей дополнительного исследования.

В работе отмечается искусственность разделения «права на доступ к информации» и «права на информацию», поскольку право на информацию вне возможностей его реализовать путем доступа к ней, теряет практический смысл.

Конституционно-правовое обеспечение безопасного обращения информации в Российской Федерации представляет собой механизм взаимодействия норм конституционного и уголовного права, в котором конституционные нормы обеспечивают общие основания для наступления уголовной ответственности, а нормы уголовного права устанавливают возможность привлечения лица к уголовной ответственности и санкции за совершенное противоправное деяние. Таким образом, рассматривая конституционно-правовое обеспечение безопасного обращения информации в Российской Федерации, подчеркивается комплексный характер данного процесса, основанного на общих положениях Конституции Российской Федерации, и конкретизированных в нормах отраслевого, в частности уголовного права.

При этом, устанавливая определенные права и обязанности в сфере информационных отношений, Конституция Российской Федерации запрещает выход за пределы очерченных прав и обязанностей, а уголовный закон (глава 28 УК РФ) определяет уголовную ответственность за невыполнение требований Конституции и законодательства РФ.

Нарушая права на безопасное обращение компьютерной информации, деятельность (действие) субъекта приобретает волевую и сознательную направленность, субъект выходит за пределы конституционно-правовых норм, посягает на основы свободного и законного информационного обмена, что влечет за собой наступление общественно опасных последствий, которые служат основанием для криминализации данного деяния либо действия.

В целом, конституционно-правовые нормы создают достаточные основания для уголовно-правовой борьбы с компьютерными преступлениями, а также формируют основы для дальнейшей криминализации деяний, посягающих на безопасное обращение компьютерной информации.

Далее автор обращается к понятию и общей характеристике преступлений против компьютерной информации по уголовному законодательству Российской Федерации. Отмечается дискуссионность понятия «преступления против компьютерной информации», отсутствие единой терминологии для обозначения преступлений в сфере информационных отношений.

Преступления против компьютерной информации – это умышленные общественно опасные деяния (действия или бездействия), причиняющие вред общественным отношениям, регламентирующим безопасное создание, хранение, использование или передачу компьютерной информации. Такие преступления обладают следующими признаками.

Во-первых, обязательным признаком данных преступлений выступает предмет – информация, представленная в форме электрических сигналов, независимо от средств ее хранения, обработки и передачи. Компьютерная информация, на которую посягает злоумышленник, может храниться либо на жестком диске компьютера, либо в сети, либо на ином носителе, но при этом она может быть использована, только посредством использования компьютерной техники.

Во-вторых, способом совершения данных преступлений всегда является модификация, несанкционированное уничтожение, блокирование, копирование, а также нейтрализация средств защиты компьютерной информации, что достигается путем целенаправленного и умышленного использования средств компьютерной техники.

В-третьих, совершение данных преступлений всегда связано с использованием средств компьютерной техники, информационных технологиями и информационно-телекоммуникационных сетей.

Наличие вышеуказанных признаков дает возможность говорить о возможности отнесения преступлений к категории составов преступлений против компьютерной информации. Термины «преступления против компьютерной информации» и «компьютерные преступления» правомерно употреблять как равнозначные (синонимы).

В зависимости от объекта и предмета все преступления, связанные с компьютерной информацией и информационно-телекоммуникационными сетями, можно разделить на две группы:

1. Преступления против компьютерной информации, в которых предметом выступает компьютерная информация (например, ст. 272-274 УК РФ).

2. Преступления, в которых компьютерная информация является орудием или средством совершения преступления. Составы таких преступлений

находятся в других разделах и главах УК РФ. Такими преступлениями, в частности, может быть мошенничество в сфере компьютерной информации (ст.159.6 УК РФ), незаконная организация и (или) проведение азартных игр с использованием информационно-телекоммуникационных сетей, в том числе сети «Интернет» (ст. 171.2 УК РФ), манипулирование рынком, то есть умышленное распространение через средства массовой информации, в том числе электронные, информационно-телекоммуникационные сети (включая сеть «Интернет»), заведомо ложных сведений или совершение операций с финансовыми инструментами, иностранной валютой и (или) товарами (ст. 185.3 УК РФ), сбыт наркотических средств, психотропных веществ или их аналогов, совершенный с использованием средств массовой информации либо электронных или информационно-телекоммуникационных сетей (включая сеть «Интернет») (ч. 2 ст. 228.1 УК РФ), фото-, кино- или видеосъемка несовершеннолетнего в целях изготовления и (или) распространения порнографических материалов с использованием информационно-телекоммуникационных сетей (включая сеть «Интернет») (ч. 2 ст. 242.2 УК РФ) и др. Существенной особенностью данных преступлений является то, что компьютерная техника не входит в число обязательных признаков состава преступлений.

В **Главе 3 «Уголовно-правовая характеристика неправомерного доступа к компьютерной информации (ст. 272 УК РФ)»** анализируются объективные и субъективные признаки данного преступления, в том числе и его квалифицированные виды.

Непосредственный объект данного преступления определяется как общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу. В числе дополнительных объектов могут быть отношения в области права собственности, в области авторского права, личные права и свободы граждан, неприкосновенность частной жизни. Наличие дополнительного объекта при совершении неправомерного доступа к компьютерной информации, как правило, влечет за собой квалификацию по совокупности с соответствующими

статьями УК РФ. Например, при неправомерном доступе, копировании и распространении компьютерной информации о частной жизни лица действия преступника будут квалифицироваться по совокупности ст. 272 и ст. 137 УК РФ.

Что касается предмета преступления, предусмотренного ст. 272 УК РФ, то им является не любая информация, находящаяся в компьютерной форме, а только охраняемая законом. Последней следует признавать информацию, к которой обладатель ограничил доступ или определил его порядок. Не является неправомерным доступ к компьютерной информации общего доступа, а именно, адресованной неограниченному кругу лиц.

В настоящее время не существует единого критерия определения ценности информации. Ценность информации правомерно определить как максимальную пользу, которую может принести данное количество информации, или как те максимальные потери, к которым приведет утрата этого количества информации. Теоретически, один и тот же информационный объект может иметь разную ценность для субъектов, в связи с чем делается вывод о том, что такая категория как «ценность информации» не может влиять на отнесение компьютерной информации к предмету преступления, предусмотренного ст. 272 УК РФ.

Под неправомерным доступом следует понимать действия, направленные на получение возможности использования компьютерной информации, которые осуществлены против воли обладателя компьютерной информации и (или) в нарушение установленного порядка доступа к ней.

Анализ последствий неправомерного доступа к охраняемой законом компьютерной информации, а именно уничтожения, блокирования, модификации либо копирования компьютерной информации позволил прийти к следующим выводам.

Наиболее опасным последствием выступает уничтожение компьютерной информации, поскольку именно оно наносит наиболее существенный, а зачастую и невосполнимый вред компьютерной информации.

Под уничтожением компьютерной информации следует понимать физическое уничтожение, при котором обладатель компьютерной информации не может ее использовать. При этом для признания воздействия на компьютерную информацию уничтожением не имеет значения, возможно ли восстановить уничтоженную информацию или нет. Не имеет значения для квалификации и то, обладает ли владелец информации копией и существует ли техническая возможность восстановления уничтоженной компьютерной информации.

Блокирование информации – это прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей). Основным признаком данного последствия является невозможность доступа к компьютерной информации со стороны законного обладателя для ее использования. При этом продолжительность блокирования должна быть достаточной, чтобы нарушить нормальную работу законного обладателя с принадлежащей ему компьютерной информацией.

Модификация компьютерной информации предполагает изменение первоначального вида представления информации (например, перестановка абзацев, строк, страниц, включение посторонних элементов, нарушение порядка расположения в базе данных). Другими словами, это внесение в компьютерную информацию изменений, которые существенно отличают ее от первоначальной (М.А. Ефремова).

Копирование компьютерной информации – это, по сути, ее перенос с одного носителя информации на другой. Дискуссионным является вопрос о том, является ли автоматическое копирование информации в оперативно-запоминающее устройство компьютера копированием информации, т.е. общественно опасным последствием неправомерного доступа к компьютерной информации, установление наличия которого является необходимым условием привлечения виновного к ответственности по ст. 272 УК РФ.

Автор приходит к выводу о том, что нельзя инкриминировать лицу, получившему доступ к компьютерной информации для ознакомления, ее

копирование по не зависящим от него обстоятельствам, связанное с особенностями компьютера и его программного обеспечения, если сохранение информации не находится в причинной связи с волеизъявлением пользователя.

Вместе с тем ознакомление с информацией путем ее прочтения не менее опасно, чем ее копирование. В некоторых случаях злоумышленнику достаточно увидеть и прочитать информацию, и она теряет свою ценность или может быть применена им в дальнейшем безо всякого копирования (Т.Л. Тропина).

В связи с этим предлагается изложить ч. 1 ст. 272 УК РФ следующим образом: «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а равно ознакомление с компьютерной информацией». Содержание термина «ознакомление», равно как и других рассмотренных выше терминов, используемых в ст. 272 УК РФ необходимо определить в специальном Постановлении Пленума Верховного Суда РФ.

Для привлечения лица к ответственности за неправомерный доступ к компьютерной информации необходимо установить наличие причинной связи между действиями виновного лица и вредными последствиями, указанными в диспозиции ст. 272 УК РФ.

Способы неправомерного доступа к охраняемой законом компьютерной информации – это совокупность приемов и методов, используемых виновным для совершения данного преступления. Неправомерный доступ может быть осуществлен двумя способами: путем хищения самих носителей компьютерной информации (например, кража диска, флеш-накопителя и т.д.) и последующего доступа к хранящейся в них компьютерной информации, либо путем перехвата информации с использованием компьютерной техники. Большинство преступлений совершается вторым способом.

Следующим факультативным признаком объективной стороны преступления, предусмотренного ст. 272 УК РФ, является место совершения неправомерного доступа к компьютерной информации. Особенностью всех

компьютерных преступлений является транснациональность (трансграничность). Они могут начать совершаться на территории одного государства, а продолжаться и закончиться на территории других государств. Кроме того, последствия, наступившие на территории одного государства, могут отражаться на территориях, находящихся под юрисдикцией других государств.

Еще одной особенностью определения места совершения преступлений в сфере компьютерной информации выступает его зависимость от способа получения доступа к компьютерной информации. Доступ к компьютерной информации может быть непосредственным, опосредованным (удаленным) и смешанным.

Время совершения компьютерных преступлений зависит от способа совершения деяния. При опосредованных и смешанных способах совершения преступления, связанных с использованием компьютерных сетей и прежде всего сети Интернет, преступники выбирают вечерние и ночные часы (с 20:00 до 4:0).

Орудиями неправомерного доступа к компьютерной информации являются, прежде всего, носители информации, а также средства преодоления защиты. Для совершения неправомерного доступа может быть задействован определенный набор орудий, которые могут быть как периферийным оборудованием, так и носителями информации.

В соответствии с ч. 1 ст. 272 УК РФ общим субъектом неправомерного доступа к компьютерной информации является вменяемое физическое лицо, достигшее 16 лет, не имеющее право доступа к компьютерной информации.

При анализе специального субъекта преступления (ч. 3 ст. 272 УК РФ) автор приходит к выводу о том, что под использованием служебного положения следует понимать использование служащими полномочий, предоставленных им в связи с занимаемой должностью, а также использование авторитета власти или занимаемого служебного положения. В данном случае это лица, которые в силу занимаемой должности или выполняемой работы

имеют доступ к компьютеру или их сети. Они могут быть законными пользователями компьютеров (программисты, сотрудники IT-отделов и т.д.), либо выполняющими абонентское обслуживание компьютеров (приходящие системные администраторы). Эти категории лиц обладают правом санкционированного доступа к компьютерной технике, но, как правило, не имеют доступа к конкретной информации, в отношении которой установлен определенный режим использования.

Интерес у исследователей проблем компьютерных преступлений вызывает криминологическая характеристика личности преступника, совершающего компьютерные преступления. Для обозначения преступников в сфере компьютерной информации предлагается использовать термин «кракер». В зависимости от цели, с которой осуществляется несанкционированный доступ к компьютерной информации, кракеров условно можно разделить три типа: «шутники», «вандалы» и «взломщики-профессионалы».

Для характеристики личности компьютерного преступления приоритетными являются такие сведения, как возраст, пол, внешность и психотип, образование и род занятий.

При анализе субъективной стороны преступления автор указывает, что неправомерный доступ к компьютерной информации совершается либо с прямым, либо с косвенным умыслом. Виновный осознает, что совершает неправомерный доступ к компьютерной информации, предвидит неизбежность или возможность наступления хотя бы одного из последствий, предусмотренных законом, желает либо сознательно допускает их наступления либо или относится к ним безразлично.

Мотивы и цели неправомерного доступа к компьютерной информации не являются обязательным признаком состава преступления. Однако, установление этих субъективных признаков позволяет выявить причины преступления, индивидуализировать ответственность, назначить справедливое наказание.

В работе обосновывается необходимость предусмотреть в качестве квалифицированного вида состава совершение деяния с целью скрыть другое преступление или облегчить его совершение (ч. 2 ст. 272 УК РФ). В данном случае автор исходит из презумпции того, что неправомерный доступ к компьютерной информации, совершенный с указанной выше целью, носит более общественно опасный характер и наносит вред владельцу информации несоизмеримо выше, чем неправомерный доступ к компьютерной информации, совершенный из хулиганских побуждений.

Говоря о квалифицированных видах неправомерного доступа к компьютерной информации, диссертант подробно останавливается на уголовно-правовой характеристике таких признаков, как «крупный ущерб», «корыстная заинтересованность», «группа лиц по предварительному сговору», «организованная группа», «тяжкие последствия».

Под крупным ущербом следует понимать невыгодные имущественные последствия обладателя компьютерной информации (например, расходы, связанные с восстановлением уничтоженного или модифицированного программного обеспечения), упущенную выгоду (например, недополученная прибыль в результате дезорганизации производственного процесса конкретного предприятия).

Корыстная заинтересованность предполагает стремление лица путем неправомерного доступа к охраняемой законом компьютерной информации извлечь выгоду имущественного характера для себя лично или для других лиц.

Исходя из смысла части 2 статьи 35 УК РФ, неправомерный доступ к охраняемой законом компьютерной информации признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступлении. При этом соглашение должно быть достигнуто до момента начала его совершения.

Следует иметь в виду, что уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации, совершенный группой лиц по предварительному сговору, наступает и в тех случаях, когда

согласно предварительной договоренности между соучастниками непосредственный доступ к компьютерной информации осуществляет один из них. Если другие участники в соответствии с распределением ролей совершили согласованные действия, направленные на оказание непосредственного содействия исполнителю в совершении преступления (например, лицо не участвовало в доступе к компьютерной информации, но по заранее состоявшейся договоренности, подстраховывало других соучастников от возможного обнаружения совершаемого преступления), содеянное ими является соисполнительством и в силу части второй статьи 34 УК РФ не требует дополнительной квалификации по статье 33 УК РФ.

Действия лица, непосредственно не участвовавшего в неправомерном доступе к охраняемой законом компьютерной информации, но содействовавшего совершению преступления советами, указаниями либо заранее обещавшего скрыть следы преступления, устранить препятствия, не связанные с оказанием помощи непосредственным исполнителям преступления, и т.п., надлежит квалифицировать как соучастие в содеянном в форме пособничества со ссылкой на часть пятую статьи 33 УК РФ.

Неправомерный доступ к компьютерной информации следует признавать совершенным организованной группой, если он совершен устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Под тяжкими последствиями надлежит понимать неправомерный доступ к охраняемой законом компьютерной информации, сопряженный с внедрением в системы, регулирующие безопасность жизни и здоровья граждан (например, в диспетчерские системы на транспорте, системы, обеспечивающие обороноспособность страны, отвечающие за экологическую безопасность), с гибелью людей либо причинением тяжкого вреда здоровью, а также со значительным экономическим ущербом государству, юридическим и физическим лицам в результате дезорганизации работы производственных

комплексов, нарушения организованной работы транспорта, уничтожения или повреждения имущества и т.п.

При этом уголовная ответственность за преступление, предусмотренное частью 4 статьи 272 УК РФ, наступает как при фактическом наступлении тяжких последствий, так и при создании угрозы их наступления. Угроза наступления тяжких последствий будет считаться созданной, если она была реальной и тяжкие последствия не наступили, лишь вследствие обстоятельств, не зависящих от воли виновного, или благодаря вовремя принятым мерам.

Предлагается de lege ferenda следующая редакция статьи 272 УК РФ:

«**Статья 272. Неправомерный доступ к компьютерной информации**

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, а равно ознакомление с содержанием компьютерной информацией, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок.

2. То же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение, –

наказывается штрафом в размере от ста тысяч до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от одного года до двух лет, либо исправительными работами на срок от одного года до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору либо лицом с использованием своего служебного положения, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они совершены организованной группой либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.

Примечания. 1. Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

2. Крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей.».

Глава 4 «Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ» состоит из трех параграфов.

Рассматривая в первом параграфе объект создания, использования и распространения вредоносных компьютерных программ неправомерного доступа к компьютерной информации, обращается внимание на то, что данное преступление является самым общественно опасным деянием из всех компьютерных преступлений. О такой позиции законодателя свидетельствует размер санкций и формальная конструкция состава данного преступления.

Под непосредственным объектом исследуемого преступления автор предлагает понимать общественные отношения, обеспечивающие право

обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

Наибольший интерес в доктрине вызывает содержание предмета преступления, предусмотренного ст. 273 УК РФ. В диссертации делается вывод о том, что в целях единства применения и толкования законодательства ст. 273 УК РФ следует дополнить примечанием следующего содержания: «Под вредоносной компьютерной программой понимается представленная в объективной форме совокупность данных и команд, предназначенных для воздействия на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящая к уничтожению, модификации, копированию, блокированию, искажению, утечке, подделке, а также к утрате, уничтожению или сбою функционирования носителя информации». В данном определении нашли бы отражения все возможные последствия, упоминаемые в действующих нормативных актах РФ.

В следующем параграфе анализируется объективная сторона преступления, предусмотренного ст. 273 УК РФ. Согласно части первой, объективной стороной выступают следующие альтернативные действия: создание, распространение или использование компьютерных программ или иной компьютерной информации, заведомо предназначенных для уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты таковой.

Под созданием вредоносных программ либо иной компьютерной информации следует понимать разработку нового вредоносного программного продукта, модификацию уже существующего продукта, следствием которых является обретение вредоносных качеств (в том числе постановку задачи, определение среды существования и цели программы; выбор средств и языков реализации программы; написание непосредственного текста программы; отладку программы; запуск и работу программы). Уголовная ответственность по статье 273 УК РФ наступает независимо от того использовалась программа

или нет, то есть само совершение перечисленных действий образуют состав оконченного преступления.

Под распространением вредоносных программ либо иной компьютерной информации следует понимать действия, направленные на получение или передачу таких программ и компьютерной информации неопределенным кругом лиц.

Использование вредоносных программ или иной компьютерной информации означает совершение любых действий по введению ее в оборот с целью достижения преступного результата. При этом нельзя признавать преступлением использование вредоносной программы для личных нужд, использование вредоносных программ организациями, осуществляющими разработку антивирусных программ.

Преступление, предусмотренное ст. 273 УК РФ, должно считаться оконченным с момента создания вредоносной программы, внесения изменений в существующие программы, использования либо распространения подобной программы.

Под нейтрализацией средств защиты информации следует понимать несанкционированное внедрение в информационную систему посредством преодоления программных средств, обеспечивающих защиту прав владельцев информации, программ, баз и банков данных от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме.

Рассматривая в следующем параграфе субъективные признаки преступления, автор отмечает, оно может быть совершено с прямым или косвенным умыслом. Решая вопрос о виновности лица, следует учитывать, что для привлечения его к уголовной ответственности не требуется наличия фактической способности компьютерной программы приводить к последствиями, предусмотренным в статье 273 УК РФ. Необходимо установить осведомленность подсудимого о вредоносности компьютерных программ.

Субъектом преступления, предусмотренного статьей 273 УК РФ, является любое физическое, вменяемое лицо, достигшее к моменту совершения преступления 16-летнего возраста, создающее, использующее или распространяющее вредоносные программы или иную компьютерную информацию.

Все вышеизложенное позволило предложить следующую редакцию статьи 273 УК РФ:

«**Статья 273. Незаконное хранение, использование, распространение и приобретение вредоносных компьютерных программ**

1. Незаконное создание, хранение, использование, распространение и приобретение компьютерной программы либо иной компьютерной информации, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, –

наказываются ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового, либо лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период от двух до трех лет

или без такового и с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, если они совершены организованной группой либо повлекли тяжкие последствия или создали угрозу их наступления, –

наказываются лишением свободы на срок до семи лет.».

Глава 5 «Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ) включает в себя четыре параграфа.

В первом параграфе, посвященном анализу объекта указанного преступления, автор приходит к выводу о том, что под ним следует понимать общественные отношения, обеспечивающие соблюдение установленных обладателем компьютерной информации правил эксплуатации средств ее хранения, обработки или передачи.

Компьютерные технологии среди прочих средств хранения, переработки и передачи информации являются наиболее удобными и прогрессивными инструментами работы с информацией. Результатом совершения этого преступления является нарушение нормальной работы технологического оборудования.

Под средствами хранения, обработки или передачи компьютерной информации диссертант предлагает понимать персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается, а также карты памяти, USB-флэшнакопители, дискеты, диски и т. п.

Исходя из положений статьи 2 Федерального закона РФ от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», информационно-телекоммуникационной сетью является технологическая система, предназначенная для передачи по линиям связи

информации, доступ к которой осуществляется с использованием средств вычислительной техники.

В соответствии со статьей 2 Федерального закона РФ от 07.07.2003 №126-ФЗ «О связи», оконченным (пользовательским) оборудованием являются технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

Норма ст. 274 УК РФ является бланкетной и для определения объективной стороны состава преступления в каждом конкретном случае необходимо определить, какие императивные положения нормативно-правовых актов были нарушены. С объективной стороны, данное деяние может выражаться как в действии, так и бездействии виновного, которые проявляются в нарушении 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.

Под нарушением правил эксплуатации следует понимать несоблюдение, ненадлежащее соблюдение, нарушение установленных правил, обеспечивающих безопасность средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям (например, эксплуатация компьютера не по прямому назначению, предоставление посторонним лицам доступа к средствам хранения, обработки или передачи охраняемой компьютерной информации, несанкционированное разглашение сетевого имени или пароля законного пользователя, нарушение температурного режима в помещении, использование нелицензионного программного обеспечения, несанкционированная замена программного обеспечения, отключение средств противовирусной защиты и др.).

Сами правила эксплуатации могут отражаться в нормативно-правовых актах или в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования либо в специальных правилах, регламентирующих особые условия (продолжительность времени, последовательность операций, максимальные нагрузки и т.д.). В последнем случае они устанавливаются производителями компьютерного оборудования и комплектующих. Кроме того, порядок использования компьютеров или их сети может устанавливаться и их собственником.

В науке выделяют два вида правил:

1) инструкции по работе с компьютерами, разработанные изготовителем компьютеров и иных электронных (цифровых) устройств;

2) правила, установленные собственником или законным пользователем информационных ресурсов, информационных систем, технологий и средств их обеспечения.

Состав преступления, предусмотренный ст. 274 УК РФ, является материальным, поскольку для признания его оконченным необходимо наступление одного из следующих последствий, перечисленных в диспозиции нормы – уничтожение, блокирование, модификация либо копирование компьютерной информации. Одновременно эти деяния должны повлечь причинение крупного ущерба. При этом наступившие последствия не должны быть результатом совершения деяний, предусмотренных ст. ст.272, 273 УК РФ.

Диссертант подчеркивает, что посредством изменений в УК РФ (Федеральный закон от 07.12.2011 № 420-ФЗ) был устранен существенный недостаток правоприменительной практики, при котором возможность привлечения виновного лица к уголовной ответственности за совершение преступления, предусмотренного ч.1 ст. 274 УК РФ зависела от субъективного взгляда правоприменителя на размер существенного вреда.

Проведенный анализ судебной практики показал, то суды при вынесении приговоров понимают под крупным ущербом расходы, которые понес

обладатель информации для восстановления нормальной работы информационных систем.

Факультативные признаки состава преступления (место, время совершения преступления) не влияют на квалификацию, но учитываются при индивидуализации наказания.

Часть 2 ст. 274 УК РФ устанавливает 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, причинившие тяжкие последствия или угрозу наступления таковых. Тяжкие последствия вследствие нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети могут выражаться и в смерти человека или причинении тяжкого вреда здоровью потерпевшего, причинении средней тяжести вреда здоровью двум потерпевшим и более, причинении легкого вреда нескольким лицам. Наиболее типичные из них: дезорганизация работы юридического лица, уничтожение, блокирование ценной информации, в том числе, и физических лиц.

Автор диссертации делает вывод о нецелесообразности декриминализации состава преступления, предусмотренного ст. 274 УК РФ, поскольку описанные в нем действия наносят серьезный ущерб обществу и государству, представляя тем самым повышенную общественную опасность.

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 охраняемой законом компьютерной информации – умышленное преступление, совершаемое с прямым или косвенным умыслом.

Субъектом преступления, предусмотренного ст. 274 УК РФ, является любое физическое, вменяемое лицо, достигшее к моменту совершения

преступления 16-летнего возраста, которое в силу характера выполняемой трудовой, профессиональной или иной деятельности имеет беспрепятственный доступ к средствам хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационным сетям и оконечному оборудованию и на которое в силу закона или иного нормативного акта возложено соблюдение соответствующих правил эксплуатации или доступа.

В **заключении** изложены основные результаты диссертационного исследования.

В **приложениях** представлены авторские редакции статей 272 и 273 УК РФ и проект постановления Пленума Верховного Суда Российской Федерации «О судебной практике по делам о преступлениях против компьютерной информации».

Основные положения диссертации отражены в следующих работах автора:

Статьи, опубликованные в ведущих рецензируемых журналах и изданиях, указанных в перечне Высшей аттестационной комиссии при Министерстве образования и науки Российской Федерации:

1. Степанов-Егиянц В.Г. Ответственность за компьютерные преступления по зарубежному законодательству / В.Г. Степанов-Егиянц // Законность. – 2005. – № 12. – С. 49-51. – 0.4 п.л.
2. Степанов-Егиянц В.Г. К вопросу о терминологии в сфере компьютерных преступлений / В.Г. Степанов-Егиянц // Черные дыры в Российском Законодательстве. Юридический Журнал «Black Holes» in Russian Legislation». – 2005. – № 4. – С. 56-64. – 0.4 п.л.
3. Степанов-Егиянц В. Г. Научно-технический прогресс в зеркале уголовной преступности / В.Г. Степанов-Егиянц // Государственная власть и местное самоуправление. — 2008. — № 11. – С. 46-48. – 0.4 п.л.

4. Степанов-Егиянц В.Г. Современная уголовная политика в сфере борьбы с компьютерными преступлениями / В.Г. Степанов-Егиянц // Российский следователь. – 2012. – № 24. – С. 43-46. – 0.3 п.л.
5. Степанов-Егиянц В.Г. Совершение кражи и мошенничества с использованием с компьютера или информационно-телекоммуникационных сетей / В.Г. Степанов-Егиянц // РИСК: Ресурсы. Информация. Снабжение. Конкуренция. – 2012. – № 4. – С. 393-396. – 0.4 п.л.
6. Степанов-Егиянц В.Г. Субъективная сторона компьютерных преступлений / В.Г. Степанов-Егиянц // Бизнес в законе. Экономико-юридический журнал. – 2013. – № 2. – С. 72-75. – 0.4 п.л.
7. Степанов-Егиянц В.Г. Объективная сторона неправомерного доступа к компьютерной информации по Уголовному кодексу РФ / В.Г. Степанов-Егиянц // Библиотека криминалиста. Научный журнал. – 2013. – № 5. – С. 42-48. – 0.5 п.л.
8. Степанов-Егиянц В.Г. Объект компьютерных преступлений в УК РФ / В.Г. Степанов-Егиянц // Библиотека криминалиста. Научный журнал. – 2013. – № 6. – С. 159-164. – 0.5 п.л.
9. Степанов-Егиянц В.Г. Информация как предмет преступления, предусмотренного ст. 272 Уголовного кодекса РФ / В.Г. Степанов-Егиянц // Законодательство. – 2013. – № 6. – С. 69-77. – 0.5 п.л.
10. Степанов-Егиянц В.Г. Характеристика субъекта неправомерного доступа к компьютерной информации по Уголовному кодексу РФ / В.Г. Степанов-Егиянц // Законодательство. – № 7. – 2014. – С. 66-73. – 0.5 п.л.
11. Степанов-Егиянц В.Г. Содержание термина «неправомерный доступ к компьютерной информации» в Уголовном кодексе РФ / В.Г. Степанов-Егиянц // Право и экономика. – 2014. – № 8. – С. 42-47. – 0.4 п.л.
12. Степанов-Егиянц В.Г. Войниканис Е.А., Машукова Е.О. Неприкосновенность частной жизни, персональные данные и ответственность за незаконные сбор и распространение сведений о

частной жизни и персональных данных: проблемы совершенствования законодательства / В.Г. Степанов-Егиянц, Е.А. Войниканис, Е.О. Машукова // Законодательство. – 2014. – № 12. – С. 74- 80. – 0.5 п.л.

13. Степанов-Егиянц В.Г. Криминологическая характеристика личности компьютерного преступника / В.Г. Степанов-Егиянц // Российский следователь. – 2014. – № 19. – С. 41-44. – 0.4 п.л.
14. Степанов-Егиянц В.Г. К вопросу об определении понятия «вредоносная компьютерная программа» в Уголовном кодексе РФ / В.Г. Степанов-Егиянц // Библиотека криминалиста. Научный журнал. – 2014. – № 6. – С. 71-75. – 0.5 п.л.
15. Степанов-Егиянц В.Г. К вопросу о предмете преступления, предусмотренного ст. 273 УК РФ / В.Г. Степанов-Егиянц // Инновации и инвестиции. – 2014. – № 9. – С. 199-202. – 0.5 п.л.
16. Степанов-Егиянц В.Г. К вопросу о месте совершения компьютерных преступлений / В.Г. Степанов-Егиянц // Научно-информационный журнал Армия и общество. – 2014. – № 5. – С. 16-19. – 0.5 п.л.
17. Степанов-Егиянц В.Г. Понятийно-терминологические основы безопасного обращения компьютерной информации в уголовно-правовом аспекте / В.Г. Степанов-Егиянц // Библиотека уголовного права и криминологии. – 2015. – № 1. – С. 118-125. – 0.4 п.л.
18. Степанов-Егиянц В.Г. Понятийно-терминологические основы безопасного обращения компьютерной информации в уголовно-правовом аспекте / В.Г. Степанов-Егиянц // Право и политика. – 2015. – № 4. – С. 592-599. – 0.5 п.л.
19. Степанов-Егиянц В.Г. Понятие «компьтерная информация» с точки зрения ее уголовно-правовой защиты / В.Г. Степанов-Егиянц // Гуманитарные, социально-экономические и общественные науки. – 2015. – № 1. – С. 171-177. – 0.6 п.л.

20. Степанов-Егиянц В.Г. Компьютерный терроризм как новая форма компьютерной преступности / В.Г. Степанов-Егиянц // Инновации и инвестиции. – 2015. – № 9. – С. 89-92. – 0.6 п.л.
21. Степанов-Егиянц В.Г. Информационная безопасность и ее уголовно-правовая защита в Российской Федерации / В.Г. Степанов-Егиянц // Инновации и инвестиции. – 2015. – № 1. – С. 171-176. – 0.5 п.л.
22. Степанов-Егиянц В.Г. Безопасное обращение компьютерной информации и проблемы международного правотворчества / В.Г. Степанов-Егиянц // Историческая и социально-образовательная мысль. – 2015. – Т. 7. – № 2. – С. 164-170. – 0.6 п.л.
23. Степанов-Егиянц В. Г. Создание, использование и распространения вредоносных программ как формы преступного посягательства на компьютерную информацию /В.Г. Степанов-Егиянц // Российский криминологический взгляд. — 2015. — № 2. — С. 316–320. – 0.5 п.л.
24. Степанов-Егиянц В. Г. Конституционные основы уголовно-правового обеспечения безопасности компьютерной информации / В.Г. Степанов-Егиянц // Современная наука: актуальные проблемы теории и практики. Серия: Экономика и право. — 2016. — № 2. – С. 161-164. – 0.4 п.л.

Монографии, статьи, научно-практические и учебные пособия:

25. Степанов-Егиянц В.Г. Уголовное право Российской Федерации: учебно-методический комплекс / Под ред. В. С. Комиссарова ; Московский государственный институт им. М.В. Ломоносова, Юридический факультет / В.Г. Степанов-Егиянц и др. – М.: Городец, 2008. – 10 п.л. Вклад автора – 0.5 п.л.
26. Степанов-Егиянц В.Г. Взаимодействие международного и сравнительного уголовного права: Учебное пособие / Отв. ред.: Комиссаров В.С.; Науч. ред.: Кузнецова Н.Ф. / В.Г. Степанов-Егиянц и др. – М.: Городец, 2009. – 9 п.л. Вклад автора – 2 п.л.

27. Степанов-Егиянц В.Г. Преступления против компьютерной информации: Сравнительный анализ / В.Г. Степанов-Егиянц. – М.: Макс Пресс Москва, 2010. – 13 п.л.
28. Степанов-Егиянц В.Г. Уголовное право Российской Федерации. Общая часть: Учебник для вузов / Под ред. В.С. Комиссарова, Н.Е. Крыловой, И.М. Тяжковой / В.Г. Степанов-Егиянц и др. – М.: Статут. 2012. – 34 п.л. Вклад автора – 0.5 п.л.
29. Степанов-Егиянц В.Г. Новая редакция статьи 274 Уголовного кодекса: проблемы и пути решения / В.Г. Степанов-Егиянц // Мониторинг правоприменения. – 2014. – № 2. – С. 18-23. – 0.4 п.л.
30. Степанов-Егиянц В.Г. Проблемы разграничения неправомерного доступа к компьютерной информации со смежными составам / В.Г. Степанов-Егиянц // Право и кибербезопасность. – 2014. – № 2. – С. 27-32. – 0.4 п.л.
31. Степанов-Егиянц В. Г. Совершение мошенничества с использованием с компьютера или информационно-телекоммуникационных сетей / В.Г. Степанов-Егиянц /// Финансовая жизнь. — 2013. — № 2. — С. 68–70. – 0.5 п.л.