МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование кафедры)

40.03.01 Юриспруденция
(код и наименование направления подготовки, специальности)

уголовно-правовой
(направленность (профиль)/специализация)

БАКАЛАВРСКАЯ РАБОТА

на тему «**ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. ПРОБЛЕМЫ КВАЛИФИКАЦИИ»**

Студент Денис Александрович Волков _____
(И.О. Фамилия) (личная подпись)

Руководитель Владимир Кузьмич Дуюнов _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой «Уголовное право и процесс»
к.ю.н., доцент С.В. Юношев _____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2019

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права

Кафедра «Уголовное право и процесс»

УТВЕРЖДАЮ
Зав. кафедрой: Юношев С.В.
_____ _____
(подпись)
«____»_____2019 г.

ЗАДАНИЕ
на выполнение бакалаврской работы

Студент Волков Денис Александрович
1. Тема «Преступления в сфере компьютерной информации. Проблемы квалификации»_____
2. Срок сдачи студентом законченной ВКР - 13 мая 2019 г.
3. Исходные данные к ВКР: Международно-правовые акты; Российское законодательство; Судебная практика; Статистический материал, собранный студентом при прохождении практики.
4. Содержание ВКР (перечень подлежащих разработке вопросов, разделов)

ВВЕДЕНИЕ

ГЛАВА 1. ЗАКОНОДАТЕЛЬСТВО ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ИСТОРИЯ И СОВРЕМЕННОСТЬ

1.1. История становления и развития российского законодательства об ответственности за компьютерные преступления

1.2. Ответственность за преступления в сфере компьютерной информации в зарубежных странах

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ

2.1. Общая характеристика преступлений в сфере компьютерной информации по Уголовному кодексу Российской Федерации

2.2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

2.3. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)

2.4. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ)

2.5. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1. УК РФ)

ГЛАВА 3. ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1. Значение термина «компьютерная информация» для квалификации компьютерных преступлений

3.2. Актуальные проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации

ЗАКЛЮЧЕНИЕ

СПИСОК ИСТОЧНИКОВ

5. Дата выдачи задания «_____»_____2019 г.

Руководитель ВКР	_____	В.К. Дуюнов
	(подпись)	(И.О. Фамилия)
Задание принял к исполнению	_____	Д.А. Волков
	(подпись)	(И.О. Фамилия)

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Тольяттинский государственный университет»

Институт права

Кафедра «Уголовное право и процесс»

УТВЕРЖДАЮ
Зав. кафедрой: Юношев С.В.
_____ _____
(подпись)
«____»_____2019 г.

КАЛЕНДАРНЫЙ ПЛАН
выполнения выпускной квалификационной работы

Студента Волкова Дениса Александровича
Тема «Преступления в сфере компьютерной информации. Проблемы квалификации»_____

Наименование раздела работы	Плановый срок выполнения раздела	Фактический срок выполнения раздела	Отметка о выполнении	Подпись руководителя
Выбор и обоснование темы ВКР	До 01 февраля 2019 г.			
Подбор библиографии	До 10 февраля 2019 г.			
Глава 1	До 1 марта 2019 г.			
Глава 2	До 31 марта 2019 г.			
Глава 3	До 25 апреля 2019 г.			
Введение	До 13 мая 2019 г.			
Заключение	До 13 мая 2019 г.			
Предварительная защита ВКР	Не позднее 20 мая 2019 г.			
Корректировка	До 15 июня			

ВКР	2019			
Защита ВКР	Не позднее 30 июня 2019			

Руководитель выпускной квалификационной работы _____ (подпись) В.К. Дуюнов (И.О. Фамилия)

Задание принял к исполнению _____ (подпись) Д.А. Волков (И.О. Фамилия)

АННОТАЦИЯ

на выпускную квалификационную бакалаврскую работу

Тема: «Преступления в сфере компьютерной информации. Проблемы квалификации».

Выпускная квалификационная работа состоит из: введения, трех глав и списка используемых источников.

Во введении обоснована актуальность выбранной темы, поставлены задачи исследования преступной деятельности в сфере компьютерной информации.

В первой главе представлена история становления и развития российского законодательства об ответственности за компьютерные преступления. Показаны этапы пути уголовно-правового регулирования вопросов ответственности за совершение преступлений в сфере компьютерной информации в Российской Федерации, а также рассмотрена уголовная ответственность за преступления в сфере компьютерной информации в зарубежных странах, так как для эффективной борьбы с преступлениями в данной сфере необходимо учитывать опыт борьбы других стран.

Во второй главе рассмотрена уголовно-правовая характеристика преступлений в сфере компьютерной информации по российскому законодательству, дана общая характеристика преступлений в сфере компьютерной информации. Произведен анализ главы 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» и произведено исследование статей 272, 273, 274, 274.1, входящих в данную главу. Рассмотрены объективные и субъективные стороны преступлений, приведены примеры ответственности за данные деяния.

В третьей главе дано определение термина «компьютерная информация», его значение для квалификации компьютерных преступлений, рассмотрены актуальные проблемы уголовно-правовой квалификации.

В заключении приведены основные выводы, полученные в результате проведенного исследования преступной деятельности в сфере компьютерной информации.

Общий объем работы составляет 72 страницы.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Актуальность выбранной темы для выпускной квалификационной работы была обусловлена чрезвычайной многогранностью и сложностью таких явления, как компьютерное преступление.

Предметами таких преступных посягательств являются сами технические средства, а также материальные объекты или программное обеспечение и базы данных, для которых само техническое средство является оружием. Компьютер может стать предметом посягательств и инструментом совершения такого рода преступления.

В наши дни быстрые способы передачи информации являются одним из самых привлекательных объектов для предпринимательской деятельности. Ежедневно они используются в коммерческих целях, тем самым приносят гигантские прибыли. Одновременно с пониманием огромной ценности информации возникает надобность в ее защите и охране. Поэтому проблема защиты компьютерной информации и информационных систем является сейчас одной из актуальных во всем нашем мире. Новые информационные технологии и доступность информации делают эту область привлекательной для представителей криминальной среды.

Для борьбы с преступлениями связанными с компьютерной информацией необходимо учитывать опыт других стран. В связи с этим, необходимо постоянно проводить мониторинг зарубежного законодательства, устанавливающего уголовную ответственность за компьютерные преступления.

Широкое использование информационно-коммуникационных технологий (ИКТ) и стремительное развитие поспособствовало переходу человечества на новую ступень развития и стало результатом революции в сфере внедрения информационных технологий.

Информационно-коммуникационные технологии трансформировали не только формы сбора и принципы, передачи информации и обработки, но они и начали оказывать мощнейшее воздействие как на экономический, так и на культурный, и политический, и даже военно-стратегический аспекты жизни

всего общества, делаясь одним из основных факторов обеспечения и поддержания устойчивого развития.

В России до 1 января 1997 года - даты вступления в действие нового УК РФ, отсутствовала возможность эффективно бороться с неправомерным доступом к компьютерной информации. Данное посягательство не было противозаконным, несмотря на явную общественную опасность, и не упоминалось нашим уголовным законодательством. Но до принятия нового УК в РФ была необходимость правовой борьбы с компьютерными преступлениями.

Количество преступлений, совершаемых в России в сфере компьютерной информации, с каждым годом неизбежно возрастает. Анализ статистических данных о преступлениях, совершенных в сфере компьютерной информации, свидетельствует, что речь идет не столько о количестве совершаемых преступлений в этой сфере, сколько о том, что при совершении других преступлений, и прежде всего экономического характера, все чаще используются информационные технологии.

Одной из важнейшей проблемы уголовно-правовых мер в обеспечении информационной безопасности выступает именно проблема, связанная с защитой информации от неправомерного доступа. Данная проблема заключается в том, что защите подлежит наиболее ценная охраняемая информация. Неправомерный доступ к охраняемой законом информации влечет опасные последствия для общества, главным образом, нарушение ее конфиденциальности, целостности, а также доступности. На сегодняшний день современные уголовно-правовые меры защиты информации от неправомерного доступа основаны на приоритетности защиты информации, которая находится на определенных носителях, и в силу несоответствия такого подхода положениям информационного законодательства, непосредственно влечет отсутствие отчетливой системы уголовно-правовой защиты информации от неправомерного доступа.

ГЛАВА 1. ЗАКОНОДАТЕЛЬСТВО ОБ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ИСТОРИЯ И СОВРЕМЕННОСТЬ

1.1. История становления и развития российского законодательства об ответственности за компьютерные преступления

Впервые преступление, совершенное на территории СССР с использованием компьютера официально зарегистрировано в 1979 году в городе Вильнюсе. Данное преступление было зафиксировано в международный реестр правонарушений подобного рода и явилось начальной точкой развития в нашей стране нового вида преступлений[1]. После этого начался поиск путей уголовно-правового регулирования вопросов ответственности за совершение таких преступлений.

В новом УК РФ появление главы 28 «Преступления в сфере компьютерной информации» подтвердило о том, что России готова принять деятельное участие в обеспечении международной законности и правопорядка. Определенные преступления в сфере компьютерной информации в главе 28 УК РФ являются уголовно наказуемыми деяниями и отнесены законодателем к посягающим на общественную безопасность и общественный порядок и размещены в раздел IX "Преступления против общественной безопасности и общественного порядка"[2].

В законе РФ «О правовой охране программ для электронных вычислительных машин и баз данных»[3] были зафиксированы важнейшие понятия и правовые конструкции. Были даны определения терминов, таких как: «программа для ЭВМ», «модификации программы», «база данных». Именно это послужило развитию правовых терминов в этой области. Закон РФ «Об ав-

[1] Батурин Ю.М., Проблемы компьютерного права. –М.: Юрид. лит., 1991.С.126.
[2] Уголовная ответственность за преступления в сфере компьютерной информации за рубежом. Лекция / Ястребов Д.А.; Под общ. ред.: Каламкарян Р.А.. -2е издание, -М.: прима-Пресс,2004. –С. 62 .
[3] Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) "О правовой охране программ для электронных вычислительных машин и баз данных". Прим. Документ утратил силу с 1 января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.

торском праве и смежных правах»[4], урегулировал отношения, которые возникают в связи с созданием и использованием произведении литературы и искусства, науки (авторское право), фонограмм, постановок, передач организаций кабельного или эфирного вещания (смежные права).

Если говорить о законе РФ «О государственной тайне»[5], данный закон урегулировал отношения, которые возникают в связи со сведениями к государственной тайне (рассекречивание и защита в интересах обеспечения безопасности Российской Федерации).

Гражданский кодекс Российской Федерации[6] в статье 128 отнес к объектам гражданских прав информацию и результаты интеллектуальной деятельности (в том числе исключительные права на них - интеллектуальная собственность).

Установлена правовая основа деятельности в области связи в законе «О связи»[7] . Определены полномочия органов госвласти по регулированию данной деятельности, а также права и обязанности как физических, так и юридических лиц, непосредственно участвующих в указанной деятельности, либо пользующихся услугами связи.

В федеральном законе РФ «Об информации, информационных технологиях и о защите информации»[8] говориться об отношениях, которые возникают:

- при использовании и формировании информационных ресурсов (в их основе создание, обработке, сборе, поиске, накопление, хранение, распространение и предоставление потребителю документированной информации);
- при создании и дальнейшего использования информационных технологий и их обеспечения;

[4] Закон РФ от 09.07.1993 N 5351-1 (ред. от 20.07.2004) "Об авторском праве и смежных правах". Прим. Документ утратил силу с 1 января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.
[5] Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.11.2011) "О государственной тайне".
[6] "Гражданский кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 06.12.2011).
[7] Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 08.12.2011) "О связи".
[8] Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 06.04.2011) "Об информации, информационных технологиях и о защите информации"

- при защите информации.

Стоит отметить, что этот закон не касается отношений, регулируемых законодательством об авторском праве и смежных правах.

Главной целью Федерального закона РФ «Об участии в международном информационном обмене»[9] является создание условий для эффективного участия России в международном информационном обмене, в едином мировом информационном пространстве. Также защита интересов Российской Федерации, субъектов Российской Федерации и муниципальных образований при международном информационном обмене, защита интересов, прав и свобод физических и юридических лиц. Данный закон ввел ряд новых определений, таких как: «информационные ресурсы», «информационные услуги», «информационные продукты», «массовая информация».

В настоящее время четко стали обозначаться проблемы применения норм 28 главы УК РФ.

В учебной и научной литературе дано большое количество определений понятия «преступления в сфере компьютерной информации», но, к сожалению, не одно из них не может дать полноты по степени обобщения[10].

По мнению многих исследователей выработался взгляд, что причиной является отсутствие общепризнанного определения «компьютерное преступление». Существует много трудностей в формулировании данного определения, так как оно должно быть достаточно емким и также достаточно специальным[11].

Отсутствие законодательного понятия «преступления в сфере компьютерной информации» затрудняется и не выполняется в полной мере применение норм о преступлениях в данной сфере.

---

[9] Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) "Об участии в международном информационном обмене". Прим. Документ утратил силу в связи с принятием Федерального закона от 27.07.2006 N 149-ФЗ.

[10] Комиссаров А. Роль криминалистики в расследовании и раскрытии компьютерных преступлений. // Конфидент. 2000. №5.С.62

[11] Панфилова Е.И., Попов А.С. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе». / Научн.ред. Волженкин Б.В. Спб.: 1998.С.11.

1.2. Ответственность за преступления в сфере компьютерной информации в зарубежных странах

Все законодательства об уголовной ответственности за преступления в сфере компьютерной информации в разных странах мира значительно отличается от законодательства Российской Федерации.

К разновидности правовых систем относится правовая семья. Правовая семья - это совокупность национальных правовых систем, к ним относятся Англо-саксонская правовая семья и Романо-германская (континентальная).

Англо-саксонская правовая система объединяет в себе две группы: группу английского права - Англия, Канада, Австралия и бывшие колонии Британской империи и право США[12].

В Соединенных штатах Америки закон о мошенничестве и злоупотреблении с использованием компьютеров был принят в 1984 году. Он образует собой основной нормативно-правовой акт, который включен в виде § 1030 в Титул 18 Свода законов США[13].

Во всех штатах США действуют также уголовные законы штатов, которыми установлена ответственность за иные преступления в рассматриваемой сфере[14].

В США рассматривается вопрос об ужесточении меры наказания за компьютерные преступления[15]. И такие шаги уже сделаны с принятием т.н. Патриотического Акта 2001 г. (США), в сфере компьютерной преступности и электронных доказательств (Computer Crime and Intellectual Property Section

[12] За исключением штата Луизиана и Калифорния, где значительную роль играют французское и испанское право. Уголовная ответственность за преступления в сфере компьютерной информации за рубежом. Лекция / Ястребов Д.А.; Под общ. ред.: Каламкарян Р.А.. - 2-е изд., перераб., доп. - М.: Прима-Пресс, 2004. – С 18.

[13] Уголовная ответственность за преступления в сфере компьютерной информации за рубежом. Лекция / Ястребов Д.А.; Под общ. ред.: Каламкарян Р.А.. - 2-е изд., перераб., доп. - М.: Прима-Пресс, 2004. – С 18.

[14] Крылова Н.Е., Серебренникова А.В. Уголовное право современных зарубежных стран (Англии, США, Франции, Германии): Учебное пособие. М.,1997. С.184-185.; Айков Д., Сейгер К., Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер.с англ. М., 1999. С.115-116.

[15] Борчева Н.А. Компьютерное право и ответственность за компьютерные преступления за рубежом. // На пути к информационному обществу: криминальный аспект. Сборник статей. М., 2002.С.15.

(CCIPS) Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001)[16].

Если говорить о Великобритании и Северной Ирландии там преступность деяний в сфере компьютерной информации установлена в 1990 году - законом «злоупотребление компьютерными средствами».

В 1997 г. был принят Закон, направленный на предупреждение преступлений обманного характера в связи с использованием телекоммуникационных систем[17], а далее закон о терроризме 2000 год[18]. Данный закон устанавливает, что незаконное проникновение в компьютеры, их системы и также сети, повлекшее за собой ущерб или использование полученной таким образом компьютерной информации для организации массовых насильственных действий, могут быть приравнены вообще к актам террора и нести за собой уголовную ответственность.

В Уголовном кодексе Австралии 1995 года[19] предусмотрен ряд статей, устанавливающих уголовную ответственность за компьютерные преступления. Расположены они в части 10.7 «Компьютерные преступления» главы 10 «Национальная инфраструктура». А в разделе 476 «Предварительные положения» определен ряд важных дефиниций.

Доступ к данным, содержащимся на компьютере может значит показ данных на дисплее компьютера или любой другой способ извлечения данных из компьютера, или копирование, или перемещение данных на любое другое место в компьютере или на устройство хранения данных, или в случае с компьютерной программой (запуск данной программы).

Санкции за серьезные компьютерные преступления от штрафа до пожизненного лишения свободы.

---

[16] Абов А.И., Ткаченко С.Н. Международный и отечественный опят борьбы с компьютерными преступлениями. М., 2004, С.7-20.

[17] Уголовное право зарубежных государств. Особенная часть: Учебн. пособие./Под ред. И предисл. Козочкина И.Д. –М, 2004. С.49-50.

[18] Terrorism Act 20th July 2000 UK Public General Acts. Закон о терроризме. http://www.legislation.gov.uk/ukpga/2000/11/contents

[19] Criminal code Australia Act No. 12 of 1995 as amended http://www.comlaw.gov.au/Details/C2011C00590

В параметрах всестороннего анализа предмета исследования уголовное законодательство европейских стран, входящих в романо-германскую (континентальную) правовую семью, также не отличается единым подходом к уголовно-правовому регулированию охраны правоотношений в сфере высоких технологий.

К романо-германской семье относятся правовые системы, возникшие первоначально в континентальной Европе на основе древнеримского права, а также канонических и местных правовых обычаев, как бы в продолжении римского права, являются результатом его эволюции и приспособления к новым условиям. Господствующая роль в таких системах принадлежит первую очередь кодексу и закону.

Одной из первых стран, предусмотревшей уголовную ответственность за компьютерные преступления, стала Швеция (Data Act, 2 апреля 1973 г.). Однако в начале 90-х годов были опубликованы материалы отчета шведских специалистов о состоянии безопасности, где было отмечено, что национальные компьютерные сети слабо защищены от случайных или преднамеренных выводов из строя[20]. Данный факт определил совершенствование уголовного законодательства в этой сфере.

По Уголовному кодексу Королевства Швеции[21] в качестве преступных признаются такие деяния, как: нарушение телекоммуникационной и почтовой тайны (ст. 8 гл. 4); мошенничество путем предоставления неправильной или неполной информации; использование технических средств, с намерением нарушить телекоммуникационную тайну (ст. 9b гл. 4).

Уголовный кодекс Голландии[22] содержит значительное количество норм об уголовной ответственности за преступления рассматриваемого вида.

В УК Голландии в статьей 80^{quinquies} введен термин «данные», и может он употребляться для обозначения всякого представления фактов, понятий

[20] Крысин А.В. Безопасность предпринимательской деятельности. М., 1996.С.172.
[21] The Swedish Penal Code 1999 http://www.sweden.gov.se/sb/d/3926/a/27777
[22] Юридическая Россия, федеральный правовой портал. Уголовный кодекс Голландии. http://law.edu.ru/norm/norm.asp?normID=1242430&subID=100100457,100100458,100100514,100101060#text

или инструкций, пригодных для передачи, толкования или обработки людьми или компьютерными приборами и системами.

В статье 80^{sexies} УК Голландии установлено, что термин «компьютерные приборы и системы» может употребляться для обозначения устройства, предназначенных для хранения и обработки данных электронными средствами.

ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ПО РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ

2.1. Общая характеристика преступлений в сфере компьютерной информации по Уголовному кодексу Российской Федерации

Преступления в сфере компьютерной информации, т.е. компьютерные преступления - это виновные посягательства, запрещенные уголовным законом, на безопасность в сфере использования компьютерной информации, причинившие значительный вред или создавшие угрозу причинения такого вреда, обществу, государству или личности.

Предметом посягательств является информация, содержащаяся в компьютере, и компьютер как информационная структура, информационный носитель. Информация - это сведения, например о лицах, предметах, фактах, событиях явлениях, содержащиеся в информационных системах. Под компьютерной информацией принято понимать информацию в оперативной памяти электронно-вычислительной машины, или на иных машинных носителях подключенных к ЭВМ, либо на съемных устройствах, включая, лазерные диски.

Название новой главы 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации» включающая в себя четыре статьи: ст.272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ», ст. 274 «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей» и ст. 247.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

Появление в Уголовном кодексе Российской Федерации в 1996 г. главы 28 было вполне обоснованным в связи с интенсивным развитием информационных технологий. Правда данная глава страдает многочисленными недостатками. Главный недостаток заключается в понятийной сфере, начиная от

отсутствия нормативного определения самого понятия компьютерной информации и заканчивая множеством спорных моментов, касательно объективной части каждой из четырех включенных в нее статей.[23]

Общественно опасные последствия преступлений в сфере компьютерной информации заключаются в: уничтожении, блокировании, модификации или копировании информации и нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Например, формально чтение информации с экрана монитора не подпадает ни под одно из выше перечисленных понятий (уничтожение, блокирование, копирование, модификация), но однако нарушает права владельца информации, к примеру, если эта информация составляет коммерческую тайну)[24].

Вполне очевидно, что мнения по поводу определения «компьютерной информации» разделились.

Например, Голубев В.А. компьютерную информацию характеризует, как «фактические данные в текстовом, графическом или ином виде, которые существуют в электронном виде, сохраняются на соответствующих носителях в форме, доступной восприятию ЭВМ или человека, либо передаваемые по телекоммуникационным каналам»[25].

К сожалению, ни в одном из действующих законодательных актов не оговаривается, каким способом, на каком виде носителя и с помощью каких технологий должна быть зафиксирована охраняемая законодательными и нормативными актами информация.

---

[23] Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. - М.: Юрист, 2009, № 5. - С. 5.

[24] Расследование неправомерного доступа к компьютерной информации: учебное пособие. Изд. 2-е, доп. И перераб. / под ред. д.ю.н., проф. Н.Г. Шурухнова. М.: Московский университет МВД России, 2004. С.95.

[25] Голубев В.А. к.ю.н., доцент, Центр исследования проблем компьютерной личности http://www.crime-research.org/library/Golu_UPK.htm

2.2. Неправомерный доступ к компьютерной информации (ст. 272 УК РФ)

В действующей редакции от 07 декабря 2011 года часть 1 статьи 272 Уголовного кодекса сообщает, что неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию, копирование компьютерной информации.

В законодательство были внесены правки для того, для решения целого ряда проблем, возникающих в правоприменительной практике. К примеру, при рассмотрении дел указанной категории, суды зачастую сталкивались с трудностями, когда неправомерный доступ осуществлялся к устройству, не подпадающему под определение ЭВМ. Например, к таким устройствам можно отнести мобильные телефоны - смартфоны).

Уголовный закон не дает четкого определения неправомерного доступа к охраняемой законом компьютерной информации, он раскрывает лишь его последствия, такие как уничтожение, блокирование, модификацию либо копирование информации. На сегодняшний день единый порядок уголовно-правового регулирования неправомерного доступа к охраняемой законом информации не установлен в действующем УК РФ. В уголовном законодательстве закреплено преступление, являющееся частным случаем неправомерного доступа к охраняемой законом информации, а именно, к неправомерному доступу к компьютерной информации.

Непосредственным объектом преступления, предусмотренного данной статьей, понимаются общественные отношения, обеспечивающие безопасность, неприкосновенность компьютерной информации[26].

Предметом преступного посягательства при неправомерном доступе к компьютерной информации является охраняемая законом компьютерная информация.

[26] Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. –М: Юристъ. 1998. –С. 549.

К примеру, так был осужден по ч. 1 ст. 272 УК РФ господин Лузгин С.Г. за неправомерный доступ к охраняемой законом компьютерной информации, который повлек ее копирование.

Согласно приговору суда, Лузгин, используя подключение к компьютерной сети Интернет через различных провайдеров, используя системный блок персонального компьютера подключенного к серверу, обеспечивающему соединение персонального компьютера с сетью Интернет, против воли сотрудника ООО «…» С., заведомо зная пароль и логин почтовой учетной записи последнего, ввел логин и пароль, тем самым совершил неправомерный доступ к почтовой учетной записи, расположенной на сервере ООО «…», а именно файлам, содержащим информацию, отнесенную обладателем к коммерческой тайне.

Так, подсудимый, указанным способом, осуществил неправомерный доступ к компьютерной информации:

- к файлу, содержащему клиентскую базу;

- к ряду файлов, содержащих информацию о коммерческом предложении агентства, которое ООО «…» готовило в рамках тендера;

- осуществил неправомерный доступ к файлу, являющемуся продуктом интеллектуальной собственности ООО «…»;

- к файлу, являющемуся презентацией креативного решения в виде эскизов макетов, описаний идей, сценариев видеороликов;

- к файлу, являющемуся продуктом интеллектуальной собственности ООО «…»;

- к файлу, содержащему информацию, относящуюся к коммерческой тайне;

- к файлу с рекламным продуктом ООО «…», которые находились на сервере организации,

и произвел копирование данных файлов на жесткий магнитный диск своего рабочего персонального компьютера.

Таким образом, господин Лузгин неправомерно осуществил доступ к охраняемой законом компьютерной информации, находящейся и хранящейся на сервере ООО «…». Он умышленно произвел копирование на жесткий магнитный диск своего рабочего персонального компьютера файлов, отнесенных к сведениям, составляющим коммерческую тайну.

Лузгин вину признал частично, указав, что около двух лет назад был трудоустроен в ООО «…» был предупрежден о сохранении коммерческой тайны, однако полагал это простой формальностью. После этого Лузгин работал на других предприятиях, а затем поступил на работу в ООО «…». Подсудимый указывает, что ООО «…» и ООО «…» прямыми конкурентами на рынке рекламных услуг не являются, поскольку занимают различные его сегменты. В период работы в ООО «…» у Лузгина имелся свой почтовый ящик, на который приходили письма. Примерно летом-осенью 2014 года Лузгин зашел на свой ящик и из любопытства проверил другие почтовые ящики, в том числе электронный почтовый ящик С., где содержалась информация, не представляющая, по мнению подсудимого, столь высокой ценности. Лузгин показал, что пароли к почтовым ящикам были простыми и подобрать их не представляло сложности, более того, многие сотрудники ООО «…» знали пароли к электронным почтовым ящикам своих коллег. Умысла на копирование информации у подсудимого не было. Лузгин полагает, что файлы могли скопироваться на жесткий диск его компьютера в момент открытия, в зависимости от настроек компьютера. Своим действиям Лузгин не придавал какого-либо серьезного значения, поскольку думал, что не совершает чего-либо противозаконного.

Суд нашел несостоятельными доводы подсудимого об автоматическом копировании компьютерной информации, которая производилась в момент прочтения Лузгиным сведений, размещенных на почтовом ресурсе С. Так, осмотром компьютерной информации, обнаруженной на рабочем компьютере Лузгина установлено, что незаконно полученная информация пересылалась подсудимым другим пользователям. Таким образом копирование охра-

няемой законом компьютерной информации производилось виновным осознанно, для целей дальнейшего использования.

Приговор Ленинского районного суда г. Екатеринбурга от 28 сентября 2015 г. по делу № 1-307/2015.

Объективной стороной преступления, предусмотренного ч. 1. ст. 272 УК РФ, выражается в неправомерном доступе к охраняемой законом информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации.

Выделяется три обязательных признака неправомерного доступа к компьютерной информации, которые характеризуют данное преступление с объективной стороны.

К примеру, так господина Сысолятин Д.А. осудили за совершение неправомерного доступа к охраняемой законом компьютерной информации по ч. 1 ст. 272 УК РФ. Совершенное им деяние повлекло блокирование и модификацию компьютерной информации.

Приказом главного врача КОГБУЗ «Нагорская ЦРБ» Сысолятин Д.А. был назначен на должность техника-программиста. Для выполнения возложенных должностных обязанностей Сысолятину Д.А. были предоставлены логин и пароль КОГБУЗ «Нагорская ЦРБ» для доступа в личный кабинет по договору оказания услуг между КОГБУЗ «Нагорская ЦРБ» и ПАО «Ростелеком».

В дальнейшем приказом главного врача КОГБУЗ «Нагорская ЦРБ» Сысолятин Д.А. был уволен с должности техника-программиста КОГБУЗ «Нагорская ЦРБ» по соглашению сторон, согласно п. 4 которого Сысолятин Д.А. обязался вернуть вверенные работодателем материальные ценности и иное имущество, в связи с чем Сысолятин Д.А. не имел права в дальнейшем осуществлять полномочия по администрированию информации.

После увольнения из КОГБУЗ «Нагорская ЦРБ» Сысолятин Д.А., преследуя личную заинтересованность, считая своё увольнение необоснованным, понимая, что в связи с прекращением трудовых отношений, он не имеет

законных оснований для доступа к охраняемой законодательством РФ компьютерной информации, принадлежащей КОГБУЗ «Нагорская ЦРБ», по мотиву неприязненных отношений с сотрудниками КОГБУЗ «Нагорская ЦРБ» и возникшим в связи с этим намерением осложнить их дальнейшую деятельность, связанную с обработкой компьютерной информации, решил осуществить неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей КОГБУЗ «Нагорская ЦРБ», содержащейся в личном кабинете КОГБУЗ «Нагорская ЦРБ» на электронном ресурсе ПАО «Ростелеком» в сети Интернет и на сервере КОГБУЗ «Нагорская ЦРБ» в виде базы данных Комплексной медицинской информационной системы (далее по тексту - КМИС).

С указанной целью Сысолятин Д.А., действуя умышленно и преследуя личную заинтересованность, используя персональный компьютер, подключенный к сети Интернет, осуществил переход на сайт (электронный ресурс), расположенный по электронному адресу: «http://j-cabinet.kirov.ru/», принадлежащий ПАО «Ростелеком». После чего, пренебрегая установленным в Российской Федерации режимом защиты персональной и компьютерной информации охраняемой законодательством РФ, Сысолятин Д.А. ввел логин и пароль от личного кабинета КОГБУЗ «Нагорская ЦРБ», предоставленные ПАО «Ростелеком» по договору оказания услуг связи, ставшие ему известными в силу ранее исполняемых им обязанностей техника-программиста. В результате указанных действий, Сысолятин Д.А. получил возможность к осуществлению модификации, блокирования, копирования и уничтожения компьютерной информации, принадлежащей КОГБУЗ «Нагорская ЦРБ».

Действуя далее, Сысолятин Д.А., управляя услугами, то есть используя содержащуюся на электронном ресурсе компьютерную информацию личного кабинета, принадлежащую КОГБУЗ «Нагорская ЦРБ», осуществил неправомерную смену паролей доступа в личный кабинет и сеть Интернет через данный личный кабинет на общий пароль «Znzwwvvv», чем модифицировал (изменил) охраняемую законом компьютерную информацию, в результате

чего, по окончании интернет-сессии, заблокировал доступ сотрудников КОГБУЗ «Нагорская ЦРБ» в сеть Интернет и к отдельным функциям КМИС, установленной на сервере КОГБУЗ «Нагорская ЦРБ», осуществляемым исключительно при наличии доступа в сеть Интернет.

Своими умышленными действиями Сысолятин Д.А. заблокировал охраняемую законом компьютерную информацию, содержащуюся в личном кабинете и на сервере КОГБУЗ «Нагорская ЦРБ» в виде базы данных КМИС, что повлекло невозможность обновления поступающей компьютерной информации и отправки в КОГБУЗ «МИАЦ» актуальных сведений об оказанных медицинских услугах в КОГБУЗ «Нагорской ЦРБ». Кроме того, умышленные действия Сысолятина Д.А. повлекли за собой невозможность предоставления КОГБУЗ «Нагорская ЦРБ» услуги электронной записи пациентов на приём к специалистам, записи пациентов специалистами на приём в другие медицинские учреждения через КМИС и ведения листов назначения.

Приговор Слободского районного суда Кировской области от 25 июля 2017 г. по делу № 1-3/17/2017.

Надо отметить, что в определении статьи указывается на неправомерный доступ именно к компьютерной информации, а не к ее носителям, где информация содержится. Из этого ясно, что физическое повреждение компьютера, ставшее причиной уничтожения информации, хранящейся на нем, не отвечает правовому содержанию общественно опасного действия, присущего преступлению, указанному в ст. 272 УК РФ и, следовательно, не образует основания для возбуждения уголовного дела за данное деяние. В данном случае речь может идти об умышленном, либо неосторожном уничтожении, либо повреждении имущества. Здесь нужно понимание направлен ли был умысел виновного именно на уничтожение информации.

К примеру именно так, была осуждена по ч. 3 ст. 272 УК РФ гражданка Воробьева Т.А. за неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной ин-

формации, совершенный лицом с использованием своего служебного положения.

Воробьева Т.А. была принята на должность специалиста по продажам корпоративным клиентам в Дальневосточный филиал - Приморское региональное отделение ПАО «...» в г. Владивостоке, и приступила к работе в указанной должности. Для работы и доступа к защищенным сетевым ресурсам ПАО «...», Воробьева Т.А. получила индивидуальный и конфиденциальный логин и пароль, составляющие ее служебную учетную запись.

Воробьева Т.А., дата, по окончании рабочего дня, действуя из иной личной заинтересованности, находясь на своем рабочем месте в офисе ПАО «...», через свой персональный компьютер скопировала из сетевых ресурсов серверов ПАО «...» информацию и сохранила на рабочем столе своего персонального компьютера в виде пяти файлов: «...» От дата.xlsb, ТОП клиенты.xls, которые в соответствии с «Заключением о степени конфиденциальности» содержат сведения, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, и составляют коммерческую тайну ПАО «...».

После чего, она умышленно действуя, осознавая фактический характер и общественную опасность своих действий, используя свое служебное положение, связанное с возможностью доступа к компьютерной информации, под своей служебной учетной записью указанные файлы поместила в созданный ею на рабочем столе защищенный паролем архив, который в качестве вложения электронного письма отправила с внешнего электронного адреса на внешний электронный адрес, которые не входили в список действующих корпоративных клиентов компании и не относились к официальным учетным записям сотрудников ПАО «...», то есть был осуществлен неправомерный доступ к охраняемой законом компьютерной информации, хранящейся в сетевых ресурсах серверов ПАО «...», что повлекло копирование указанной информации.

Приговор Фрунзенского районного суда г. Владивостока от 21 сентября 2018 г. по делу № 1-318/2018.

В статье 272 УК РФ есть некоторые смысловые и терминологические противоречия. Признаками объективной стороны неправомерного доступа к компьютерной информации являются последствия в виде: уничтожения, блокирования, модификации или копирования компьютерной информации. Чтение информации - это самое простое, распространенное и опасное деяний, которое не вошло в перечень неправомерного доступа. В случаях, когда речь идет о государственной, банковской, коммерческой и профессиональной тайнах такое действие вполне может являться оконченным преступлением. И несмотря на то, что статья имеет название «Неправомерный доступ к компьютерной информации», она все же не содержит каких-либо санкций за неправомерный доступ к таковой. А ответственность по ней наступает лишь в случае, если этот доступ повлек: уничтожение, блокирование, модификацию, копирование информации. Проанализировав статью, можно подчеркнуть, что чтение информации, охраняемой законом, преступлением не является. Совершенно очевидно, что во многих случаях злоумышленнику вполне достаточно узнать какие-либо сведения (к примеру, сведения о количестве денег на счету партнера или конкурента – банковскую тайну и т.п.).

Так, приговором суда было установлено, что у Овчинникова С.О., имевшего при себе пластиковую банковскую карту «Maestro» Сбербанка России, оформленную на Потерпевшего № 1, которую в один из дней начала апреля 2016 года Потерпевший № 1 добровольно передал Овчинникову С.О. во временное пользование, сказав при этом «пин - код» от данной банковской карты, возник преступный умысел на совершение тайного хищения денежных средств с лицевого счета Потерпевшего №1 вышеуказанной банковской карты.

Реализуя свой преступный умысел, направленный на тайное хищение денежных средств, принадлежащих Потерпевшему № 1 с банковской карты «Maestro» Сбербанка России, Овчинников С.О. в вышеуказанный период

времени, действуя умышленно из корыстных побуждений, с целью тайного хищения чужого имущества, с целью извлечения имущественной выгоды, путем свободного доступа , осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно-опасных последствий в виде причинения значительного материального ущерба Потерпевшему №1 и желая их наступления, решил, предварительно завладеть персональными средствами доступа к системе «Сбербанк онлайн» (идентификатор, постоянный и одноразовые пароли), с помощью системы «Сбербанк онлайн» и осуществлять операции по переводу денежных средств со счета банковской карты «Maestro» Сбербанка России, оформленной на Потерпевшего №1, тем самым похитить денежные средства Потерпевшего №1, находящиеся на его лицевом счете банковской карты.

После чего, Овчинников С.О., находясь в помещении, где расположен банкомат Сбербанка России, без ведома Потерпевшего №1, с помощью банкомата подключил к банковской карте «Maestro» Сбербанка России, оформленной на Потерпевшего №1, банковские услуги «Мобильный банк» и «Сбербанк онлайн» к сотовому телефону с абонентским номером, находящегося в пользовании Р. Таким образом, Овчинников С.О. получил идентификатор, постоянный и одноразовые пароли к персональным средствам доступа к системе «Сбербанк онлайн» по банковской карте Потерпевшего №1 с целью последующего контроля баланса банковской карты последнего и перевода с его банковской карты денежных средств, при этом Овчинников С.О. переписал идентификатор и постоянный пароль на обложку тетради и оставил ее себе.

Далее, Овчинников С.О. с помощью находящегося у него нетбука, подключенного к сети «Интернет», зашел в систему «Сбербанк онлайн», подключенной к вышеуказанной банковской карте Потерпевшего №1, где с помощью находящегося у него ранее полученного идентификатора и постоянного пароля, осуществил доступ к личному кабинету системы «Сбербанк онлайн» Потерпевшего №1, содержащему сведения о его банковских счетах

(картах), остатках денежных средств на счете и проверил баланс банковской карты Потерпевшего №1, на балансе банковской карты которого находились денежные средства в сумме 8471 руб. 80 коп. После этого Овчинников С.О. перевел в системе «Сбербанк онлайн» с лицевого счета банковской карты Maestro» Сбербанка России, оформленной на Потерпевшего №1, на лицевой счет своей банковской карты «Maestro» Сбербанка России денежные средства в сумме 8400 руб., принадлежащие последнему.

Далее, Овчинников С.О., находясь в помещении, где расположен банкомат Сбербанка России, обналичил со своей банковской карты «Maestro» Сбербанка России денежные средства в сумме 8400 руб., которые ранее перевел с лицевого счета Потерпевшего №1 вышеуказанной банковской карты.

В судебном заседании государственный обвинитель просил исключить из предъявленного Овчинникову С.О. обвинения, как излишне вмененные ч. 3 ст. 183 УК РФ, ч. 2 ст. 272 УК РФ, поскольку согласно материалам уголовного дела, умысел подсудимого был направлен на хищение денежных средств потерпевшего и получение сведений о пароле от системы автоматизированного облуживания клиентов «Сбербанк онлайн», доступ к указанной системе, являются способом совершения преступления.

Суд, соглашаясь с мнением государственного обвинителя, исключает из обвинения, предъявленного Овчинникову С.О., как излишне вмененные ч. 3 ст. 183 УК РФ, ч. 2 ст. 272 УК РФ.

Приговор Козельского районного суда Калужской области от 08.05.2018 по делу № 1-1-57/2018.

Важным остается установление причинной связи между несанкционированным доступом и наступлением последствий. При функционировании сложных компьютерных систем возможно уничтожение, блокирование в результате технических неисправностей, либо программных ошибок. Ответственность по ст. 272 УК РФ наступает только в том случае, если преступные последствия, альтернативно отраженные в ее диспозиции. Явились именно необходимым следствием, закономерно вызванным неправомерным досту-

пом лица к охраняемой законом компьютерной информации, а не наступили в силу иных причин. Данное преступление считается оконченным в момент наступления предусмотренных в ст. 272 УК РФ последствий, то есть все действия, выполненные до формальной подачи последней команды, будут образовывать состав неоконченного преступления.

Так, Щербак Е.Д. был признан виновным в совершении преступления, предусмотренного ч. 3 ст. 30 и ч. 1 ст. 272 УК РФ, покушение на неправомерный доступ к охраняемой законом компьютерной информации и повлекший копирование компьютерной информации, при следующих обстоятельствах.

Согласно приговору, Щербак Е.Д. работал в представительстве ООО «***» главным специалистом – координатором, затем исполнял обязанности директора представительства. Впоследствии Щербак Е.Д. был уволен из ООО «***» по собственной инициативе.

В период работы в представительстве ООО «***» Щербак Е.Д. имел доступ к конфиденциальной информации, в том числе к базам данных, содержащим персональные данные должников, имел персональную электронную почту, которой пользовался в период работы.

После увольнения из ООО «***», Щербак Е.Д. трудоустроился в «***» где по роду своей деятельности был связан с выдачей физическим лицам займов, и персональные данные лиц, являвшихся неплательщиками по долгам, имели значение для его профессиональной деятельности

В связи с этим у Щербака Е.Д. возник преступный умысел на незаконное получение реестров должников ООО «***», то есть на неправомерный доступ к охраняемой законом компьютерной информации, принадлежащей ООО «***», с ее копированием.

Для осуществления задуманного Щербак Е.Д. решил в служебном помещении представительства ООО «***», используя для доступа в систему учетную запись и пароль, предоставленные ему ООО «***» в период его работы, осуществить выход в корпоративную локальную сеть ООО «***» на

ранее используемый им электронный почтовый ящик, откуда осуществить копирование реестров должников ООО «***», отправив их по электронной почте на внешние электронные почтовые ящики, используемые им в личных целях.

С целью реализации преступного умысла он приехал в административное помещение представительства ООО «***», и проследовал в служебный кабинет, который находился на первом этаже. Воспользовавшись дружескими отношениями с работником представительства ООО «***» Свидетелем 1, находившемся в указанном кабинете, Щербак Е.Д. занял рабочее место за одним из столов, на котором находился монитор и «тонкий клиент», подключенный к локальной сети ООО «***». Осуществляя умысел, Щербак Е.Д. неправомерно включил указанный компьютер, затем используя ранее имеющуюся у него учетную запись с данными (логином и паролем), известным только ему, которые, несмотря на прекращение трудовой деятельности Щербака Е.Д. в ООО «***», являлись действующими. Он вошел в локальную компьютерную сеть ООО «***», а затем вошел в электронный почтовый ящик, ранее используемый им, и создал электронное письмо, и прикрепил к нему файлы, которые находились в сетевом ресурсе ООО «***», и содержащие охраняемую законом информацию о персональных данных о личности. Также к указанному сообщению Щербак Е.Д. прикрепил файлы, содержащие информацию, не охраняемую законом.

Указанное письмо и файлы ушли на его электронный почтовый ящик. Тогда же с целью получения указанной информации, для обеспечения большей надежности ее получения Щербак Е.Д. решил оправить на другой электронный почтовый ящик еще несколько электронных сообщений с вложенными файлами, содержащими персональные данные о личности.

Находясь в программе с синхронизированным электронным почтовым ящиком, Щербак Е.Д. создал электронное письмо, и прикрепил файлы, которые находились в сетевом ресурсе ООО «***», содержащие охраняемую законом информацию о персональных данных о личности. Данное письмо и

файлы Щербак Е.Д. отправил на электронный почтовый ящик с адресом ресурса в сети Интернет, находящегося за пределами Российской Федерации. При этом Щербак Е.Д., имея электронный почтовый ящик с адресом на электронном ресурсе в сети Интернет, находящемся за пределами Российской Федерации, ошибочно указал неверный адрес электронного почтового ящика на электронном ресурсе gmail.ru в сети Интернет, и оправленное им сообщение со всеми вложениями заведомо не могло быть доставлено, что на тот момент Щербак Е.Д. не обнаружил.

С той же целью в программе с синхронизированным электронным почтовым ящиком Щербак Е.Д. создал еще два электронных сообщения, к которым прикрепил файлы, находившиеся на сетевом ресурсе ООО «***», содержащие информацию о персональных данных о личности охраняемую федеральным законом. Также к указанным сообщениям Щербак Е.Д. прикрепил файлы, содержащие информацию, не относящуюся к охраняемой законом, и вновь отправил на несуществующий электронный почтовый ящик на электронном ресурсе в сети Интернет.

Всеми совершенными действиями Щербак Е.Д. осуществил неправомерный доступ к охраняемой законом компьютерной информации. Совершил действия, непосредственно направленные на ее копирование, которое Щербаку Е.Д. осуществить не удалось, поскольку в соответствии с настройками локальной сети ООО «***» отправка электронных писем на почтовый сервер запрещена, о чем Щербак осведомлен не был, а почтовый ящик с адресом «данные изъяты» на электронном ресурсе в сети Интернет «данные изъяты» ru не был зарегистрирован Щербаком Е.Д., и электронные письма, отправленные им на этот электронный ящик, доставлены быть не могли, о чем Щербак Е.Д. на тот момент осведомлен не был.

Тем самым, Щербак Е.Д. осуществил неправомерный доступ к охраняемой Федеральным законом «О персональных данных» от 27 июля 2006 г. N 152-ФЗ и Указом Президента Российской Федерации от 6 марта 1997 года № 188 "Об утверждении перечня сведений конфиденциального характера" ком-

пьютерной информации, владельцем которой являлось ООО «***», содержащей персональные данные о личности должников ООО «***»», совершил умышленные действия, непосредственно направленные на копирование данной информации, однако, не смог окончить преступление по независящим от него причинам.

Приговор Октябрьского районного суда г. Саратова от 26.02.2014 по делу № 1-27/2014.

Часть 2 статьи 272 УК РФ гласит, что то же деяние, причинившее крупный ущерб или совершенное из корыстной заинтересованности (крупным ущербом в статьях настоящей главы признается ущерб, сумма которого превышает один миллион рублей).

Часть 3 статьи 272 УК РФ рассматривает деяния, предусмотренные частями первой или второй настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения. Часть 4 статьи 272 Уголовного кодекса рассматривает деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления.

В примечании к данной статье раскрываются понятия компьютерной информации и размера крупного ущерба. Во-первых компьютерная информация – это сведения или сообщения, или данные, которые представлены в форме электрических сигналов, независимо от средств их хранения, обработки или её передачи. А во-вторых крупным ущербом в статьях данной главы признается ущерб, где сумма которого превышает один миллион рублей[27].

Так, Евсеев А.А. был осужден за неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее блокирование по ч. 2 ст. 272 УК РФ. Согласно приговору суда Евсеев А.А. при настройке персонального компьютера К. случайно получил зарегистрированные за ним иденти-

[27] Уголовный кодекс Российской Федерации от 13.06.1996 №63-ФЗ (ред. 23.04.2019). Ст.272 «Неправомерный доступ к компьютерной информации».

фикационные данные о сетевых реквизитах, которые скопировал на жесткий диск персонального компьютера своей супруги Е.

Евсеев А.А., руководствуясь корыстными побуждениями, обусловленными желанием получения бесплатной услуги доступа к сети Интернет, осознавая, что несанкционированное использование им сетевых реквизитов без разрешения их законного владельца К. нарушит установленный законодательством РФ порядок получения услуги доступа к сети Интернет, и, относясь безразлично к наступлению общественно-опасных последствий в виде блокирования доступа к данной информации законному абоненту, не поставив Е. в известность о своих преступных намерениях, настроил указанную учетную запись в разделе «сетевые подключения» панели управления операционной системы ЭВМ для установления VPN-соединения в автоматическом режиме с сервером провайдера. Реализуя заранее обдуманный преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, Евсеев А.А. с помощью находящегося в его пользовании персонального компьютера, использовал зарегистрированные на имя К. идентификационные данные (логин и пароль) для соединения с сервером оператора связи, посредством которого осуществил 275 неправомерных подключений к глобальной сети Интернет.

Всего продолжительность неправомерных подключений к глобальной сети Интернет, осуществленных Евсеевым А.А. через сервер, составила 468 491 секунду (130 часов 08 минут 11 секунд). В результате неправомерного доступа к охраняемой законом компьютерной информации в течение указанного времени доступ к сети Интернет законному пользователю информации К. был заблокирован.

Приговор Магаданского городского суда Магаданской области от 28.05.2013 по делу № 1-351/2013.

Неправомерный доступ к компьютерной информации – умышленное деяние, поскольку в диспозиции ст. 272 УК РФ не указано обратное. Человек, пытающийся получить доступ к информации, должен сознавать, что свобод-

ный доступ к информации ограничен, он не имеет прав на доступ к этой информации. Об умысле будут свидетельствовать меры защиты информации от доступа посторонних (коды, пароли и т.п.), которые приходится преодолеть. Чтобы получить доступ к информации, вывод на экран дисплея компьютера предупреждающих сообщений, устные уведомления о запрете доступа к информации и т.д. Но закон вовсе не ограничивает привлечение лица к уголовной ответственности по данной статье в случае совершения этого преступления с косвенным умыслом. Как показывает практика, преступник не всегда желает наступления вредных последствий. Особенно это характерно при совершении данного преступления из озорства или так называемого спортивного интереса.

Так, Богдановский А.В. был осужден по ч. 1 ст. 272 УК РФ за неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Согласно приговору суда у Богдановского А.В. из хулиганских побуждений возник преступный умысел, направленный на неправомерный доступ к компьютерной информации своего знакомого А.А.В., содержащейся в электронном почтовом ящике последнего, то есть к охраняемой информации. В связи с тем, что электронный почтовый ящик, а также содержащаяся в нем информация являются собственностью А.А.В., пароль Богдановскому А.В. известен не был. Однако Богдановскому А.В. был достоверно известен адрес электронного почтового ящика, и он знал, что для получения указанного пароля необходимо предоставить персональные данные А.А.В., которые ему были хорошо известны в силу их длительного знакомства.

Богдановский А.В., находясь у себя дома, действуя умышленно, из хулиганских побуждений, для входа в электронный почтовый ящик, принадлежащий А.А.В., используя свой персональный компьютер, к которому подключено оборудование для выхода в «Интернет» вошел в интернет-проводник «Джимайл», ввел адрес электронной почты А.А.В. «Саратов.рем

собака джимайл.ком» и для получения пароля обратился к администратору проводника. В результате данного обращения администратором интернет-проводника Богдановскому А.В. было предложено ввести персональные данные А.А.В., а именно: дату рождения и логин, которым являлся абонентский номер мобильного телефона А.А.В. Предоставив персональные данные А.А.В., Богдановский А.В. получил пароль и совершил неправомерный доступ к компьютерной информации А.А.В., содержащейся в электронном почтовом ящике.

Не остановившись на достигнутом, Богдановский А.В. совершил копирование информации, содержащейся в почтовом электронном ящике А.А.В. на свой персональный компьютер, а также ее частичное уничтожение, после чего совершил модификацию и блокирование компьютерной информации А.А.В. путем изменения пароля, необходимого для входа в электронный почтовый ящик.

Данный приговор вынес Энгельский районный суд Саратовской области от 15.08.2016 по делу № 1-504/2016.

Интеллектуальный момент вины, характерный для состава анализируемого преступления, заключается в осознании виновным факта осуществления неправомерного доступа к охраняемой законом компьютерной информации. При этом виновный понимает не только фактическую сущность своего поведения, но и его социально опасный характер. Кроме того, виновный предвидит возможность или неизбежной реального наступления общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования информации. Следовательно, субъект представляет характер вредных последствий, осознает их социальную значимость и причинно-следственную зависимость.

Так, приговором суда было установлено, что Сокирко С.Г. с использованием своего служебного положения совершила нарушение тайны телефонных переговоров граждан, а также неправомерный доступ к охраняемой за-

коном компьютерной информации, что повлекло копирование компьютерной информации.

Сокирко С.Г. была назначена на должность старшего продавца-консультанта салона связи. При заключении трудового договора Сокирко С.Г. дала обязательство соблюдать конфиденциальность и воздерживаться от разглашения, предоставления доступа, выдачи или иных способов передачи данных и информации (в том числе устного их разглашения или каких-либо высказываний в связи с ними), которая имеется в ее распоряжении или станет ей известна в процессе работы или в связи с выполнением должностных обязанностей какой-либо третьей стороне или лицам, которые не должны иметь доступа к таким данным, а также была предупреждена об уголовной ответственности по ст. 138 и ст. 272 УК РФ.

Сокирко С.Г., реализуя единый с неустановленным следствием лицом преступный умысел, направленный на нарушение тайны телефонных переговоров З.Е.В. и неправомерный доступ к охраняемой законом компьютерной информации с использованием служебного положения группой по предварительному сговору, находясь на своем рабочем месте в салоне связи, осознавая общественную опасность и преступный характер совершаемых ею действий, предвидя наступление общественно опасных последствий в виде нарушения тайны телефонных переговоров З.Е.В., и желая их наступления, будучи обязанной соблюдать меры безопасности, направленные на защиту конфиденциальности информации абонентов, используя свое служебное положение, свой логин и пароль, в отсутствие судебного решения и иных законных оснований, умышленно сформировала заявку на получение детализации телефонных соединений абонента З.Е.В., а именно ввела в информационно-биллинговую систему SBMS абонентский номер, произвела регистрацию не имевшего места в действительности обращения З.Е.В., тип услуги – «детализация счета», выбрала период получения детализации и прикрепила к заявке в электронном виде (формате «PDF») заявление, якобы полученное от З.Е.В. В результате обработки заявки на получение детализации телефонных

соединений абонента, последняя была сформирована и направлена системой в виде файла формата «PDF» на локальный персональный компьютер салона связи, в котором запрошена детализация, с идентификатором, что повлекло копирование компьютерной информации на указанный компьютер.

После чего Сокирко С.Г., продолжая реализовывать единый с неустановленным следствием лицом преступный умысел, направленный на нарушение тайны телефонных переговоров и неправомерный доступ к охраняемой законом компьютерной информации с использованием служебного положения группой по предварительному сговору, произвела незаконное копирование детализации телефонных соединений абонента путем ее фотографирования и, при помощи приложения для смартфонов «VIBER», направила копию данной детализации неустановленному следствием лицу, чем нарушила конституционное право З.Е.В. на тайну телефонных переговоров.

Приговор Советского районного суда г. Краснодара от 27.07.2016 по делу № 1-481/16.

Мотивы и цели данного преступления могут быть разными. Это может быть и корыстный мотив, и месть, и цель получить какую-либо информацию, может быть желание причинить вред или желание проверить свои профессиональные способности, а также самоутвердиться.[28]

2.3. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ)

Часть 1 статьи 273 Уголовного кодекса гласит, что создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации наказуемо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же

[28] Постатейный Комментарий к Уголовному кодексу РФ. / Под ред. Наумова А.В. –М., 1998.

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

Часть 2 статьи 273 Уголовного кодекса предусматривает ответственность за деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности.

В части 3 изложена ответственность за деяния, предусмотренные частями первой или второй настоящей статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. Санкция данной нормы предусматривает наказание в виде лишения свободы на срок до семи лет[29].

Статья 273 УК РФ обусловлена ответственностью за создание и распространение разного рода компьютерных программ - «вирусов», которые могут повреждать информацию, а также нарушить штатную работу компьютера. Данная статья защищает права владельца компьютерной системы на неприкосновенность и целостность, находящиеся в ней информации[30]. «Вредоносная программа» схожа с понятием «программа-вирус».

Объективные признаки создания, исполнения и распространения вредоносных компьютерных программ указаны в ст. 273 УК РФ. Объект - правоотношения в сфере обеспечения безопасности сбора, поиска, хранения, обработки , передачи, накопления, распространения и потребления компьютерной информации, использования информационных компьютерных технологий, защиты компьютерной информации. Под предметом рассматривается вид преступных посягательств – «программы вредоносные».

[29] "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 23.04.2019)

[30] Галкин А.И. Уголовная ответственность за преступления в сфере компьютерной информации // Следователь. Федеральное издание. - М., 2009, № 5 (133). - С. 6.

Объективная сторона это создание программ заведомо портящих информации, нарушающих работу, а равно в использовании распространении таких программ или машинных носителей.

Общее понятие «программы вредоносные» обозначает программы, кем то намеренно созданные для нарушения работы компьютерных программ.

К наиболее распространенным видам вредоносных программ можно отнести: «компьютерные вирусы»; «троянские кони»; «логические бомбы.

Вредоносность программ в целом определяется ее назначением и способностью уничтожать, модифицировать, блокировать, копировать информацию.

Вредоносной считается программа, если она вызывает самопроизвольное уничтожение, блокирование, модификацию, копирование компьютерной информации.

В данной статье УК РФ идет речь не только о программах, записанных на машинных носителях, но и о записях программ на бумажном виде. Обусловлено это тем, что процесс создания программы для компьютерных устройств зачастую начинается написанием ее текста с последующим введением его в память устройства или без такового. С этим учетом наличие исходных текстов с написанием вирусных программ является основанием для привлечения к ответственности по ст. 273 УК РФ.

Внесение изменений в существующую программу вполне может быть элементом объективной стороны преступления, но лишь в том случае, если исправление внесены в работающую программу, либо программа с внесенными изменениями распространена на любом носителе машинной информации. А вот исправление написанной программы на бумаге само по себе не подразумевается данной нормой уголовного закона, в случае если этот бумажный вариант не будет непременно использован для распространения.

Части 2 и части 3 ст. 273 УК РФ представляют собой квалифицированные составы деяния, описанного в первой части указанной статьи (простого состава).

В первой части определены способы совершения преступления "Создание, распространение или использование" компьютерных программ и иной компьютерной информации. Лицо будет считаться совершившим преступление, если удастся доказать, что оно знало о том, что программы предназначены "для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации...", а программы несомненно должны действительно обладать подобными свойствами.

К тяжким последствиям, наступление которых является квалифицирующим признаком ч. 3 ст. 273 УК РФ, могут быть отнесены безвозвратная утрата особо ценной информации, выход из строя важных технических средств, повлекших гибель людей, аварии, дезорганизацию производства и т.д.[31]

Так, подсудимый Рыжов А.Н. совершивший деяние по распространению компьютерных программ, предназначенных для несанкционированного уничтожения, модификации компьютерной информации.

Согласно приговору суда в 2012 году Рыжов А.Н. вступил в состав созданной лицом 1 организованной группы, целью создания которой являлось осуществление преступной деятельности, связанной с созданием, распространением и использованием на автозаправочных комплексах ОАО «Воронежнефтепродукт» вредоносного программного обеспечения, предназначенного для систематического недолива топлива, отпускаемого клиентам, а также реализации нефтепродуктов клиентам в отсутствии контрольно-кассового учета.

Рыжов А.Н., являясь членом организованной группы, зная специфику работы сети автозаправочных комплексов ОАО «НК «Роснефть», действуя во взаимодействии с лицом №6, лицом №5, (ФИО25) и (ФИО6) осуществлял распространение вредоносного программного обеспечения, в частности:

[31] Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. - М.: Юрист, 2002, № 9. - С. 39

- в целях сокрытия преступной деятельности от правоохранительных органов использовал криптографические средства шифрования информации при обмене с (ФИО25) текстовыми СМС сообщениями по вопросам времени и места встречи с (ФИО25) и (ФИО6) в г. Воронеж и Воронежской области для следования к АЗК ОАО «Воронежнефтепродукт» и перепрограммирования электронных блоков топливораздаточных колонок марки «Scheidt&Bachmann»;

- информировал лицо №5 о времени выезда, месте встречи на территории Белгородской области для следования в г. Воронеж и Воронежскую область для осуществления перепрограммирования электронных блоков топливораздаточных колонок марки «Scheidt&Bachmann» на АЗК ОАО «Воронежнефтепродукт»;

- вместе с лицом №5 присутствовал во время проводимых им манипуляций по перепрограммированию электронных блоков топливораздаточных колонок марки «Scheidt&Bachmann» на АЗК ОАО «Воронежнефтепродукт», в пределах полученных знаний и опыта, участвовал в процессе извлечения электронных блоков и их перепрограммирования;

- получал от представителя ОАО «Воронежнефтепродукт» и активного члена организованной группы лица №4 денежные средства в качестве платы за перепрограммирование электронных блоков топливораздаточных колонок марки «Scheidt&Bachmann» на АЗК ОАО «Воронежнефтепродукт»;

- в качестве гонорара передавал лицу №5 часть денежных средств, вырученных в результате перепрограммирования электронных блоков топливораздаточных колонок марки «Scheidt&Bachmann» 27 АЗК ОАО «Воронежнефтепродукт».

Массовое использование в сети автозаправочных комплексов ОАО «Воронежнефтепродукт» вредоносного программного обеспечения, предназначенного для недолива топлива клиентам и его бесконтрольной реализации создало угрозу наступления тяжких последствий принадлежащему Российской Федерации предприятию, что выразилось в подрыве уровня доверия

клиентов к деятельности автозаправочных комплексов ОАО «Воронежнефтепродукт», как следствие снижение прибыли ОАО «Воронежнефтепродукт» за 2014 год на сумму не менее 150 млн. руб. от прогнозируемой, а также лишило экономического эффекта затраты за 2013 и 2014 года на сумму 21,18 млн. руб., направленные на повышение продаж за счет укрепления уровня доверия клиентов.

Приговор Коминтерновского районного суда г. Воронежа от 24.04.2017 по делу № 1-271/2017.

Субъективные признаки создания, использования и распространения вредоносных компьютерных программ.

Субъект данного преступления - общий, т.е. субъектом преступления может быть любое вменяемое лицо, достигшее возраста 16 лет.

Когда действие вредоносной программы необходимо для совершения другого преступления, содеянное подлежит квалификации по совокупности вне зависимости от степени тяжести другого преступления.

Так, у Сокольникова В.Ю. в целях облегчения совершения другого преступления, а именно неправомерного доступа к компьютерной информации, возник умысел использовать вредоносные программы, с помощью которых внеси изменения в системные программные обеспечения указанных игровых устройств, блокировав действия встроенной защиты от воспроизведения неавторизированного контента. С этой целью Сокольников В.Ю. из сети «Интернет» скачал специализированное программное обеспечение, являющееся вредоносной и осуществляющее блокировку, модификацию и уничтожение средств защиты информации игровой приставки и одновременно с этим в «Интернет-магазине» приобрел элементный модуль - «чип», в постоянном запоминающем устройстве которого содержится программа, являющаяся вредоносной и осуществляющая блокировку, модификацию и уничтожение средств защиты информации игровых консолей..

После этого, желая получить возможность воспроизведения на игровой приставке и игровой консоли неавторизированных производителем игровых

программ, Сокольников В.Ю., осознавая, что он использует специальные устройства («...»-программаторы) и специализированное программное обеспечение (разновидность программ «NandPro»), основным назначением которого является изменение внутреннего системного программного обеспечения игровой приставки, которое блокирует встроенную программную техническую защиту игровых приставок и изменяет алгоритм работы, а также используя модуль, в постоянном запоминающем устройстве которого содержится программа, блокирующая действие встроенной защиты игровых консолей, то есть осуществляет блокировку, модификацию и уничтожение средств защиты информации, внес изменения в системное программное обеспечение игрового устройства, что позволило заблокировать предусмотренные производителем средства защиты компьютерной информации и получить возможность использования неавторизированного программного обеспечения.

Кроме того он же совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекшее уничтожение, блокирование, модификацию компьютерной информации, а также совершил использование компьютерных программ заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, компьютерной информации или нейтрализации средств защиты компьютерной информации, из корыстной заинтересованности.

Суд учел, что Сокольников В.Ю. впервые совершил умышленные преступления небольшой и средней тяжести и назначил ему наказание в виде ограничения свободы по каждому преступлению. Окончательное наказание подсудимому суд назначил по правилам ч. 2 ст. 69 УК РФ путем поглощения менее строгого наказания более строгим.

Приговор Октябрьского районного суда г. Саранска Республики Мордовия от 29 января 2015 г. по делу № 1-310/2014.

В настоящее время квалификация действий программиста должна производиться по ч.1 ст. 273 УК РФ..

Приговором Коминтерновского районного суда г. Воронежа от 24.04.2017 по делу № 1-271/2017 было установлено, что массовое использование в сети автозаправочных комплексов ОАО «Воронежнефтепродукт» вредоносного программного обеспечения, предназначенного для недолива топлива клиентам и его бесконтрольной реализации создало угрозу наступления тяжких последствий принадлежащему Российской Федерации предприятию, что выразилось в подрыве уровня доверия клиентов к деятельности автозаправочных комплексов ОАО «Воронежнефтепродукт», как следствие снижение прибыли ОАО «Воронежнефтепродукт» за 2014 год на сумму не менее 150 млн. руб. от прогнозируемой, а также лишило экономического эффекта затраты за 2013 и 2014 года на сумму 21,18 млн. руб., направленные на повышение продаж за счет укрепления уровня доверия клиентов.

Преступление совершается с двумя формами вины, то есть характеризуется умыслом относительного факта создания, использования или распространения вредоносной программы и неосторожностью (легкомыслием либо небрежностью) относительно наступления тяжких последствий. Это означает, что причинение тяжких последствий не охватывается умыслом виновного, однако он предвидит возможность их наступления, но без достаточных к тому оснований самонадеянно рассчитывает на их предотвращение, либо не предвидит, хотя должен был и мог предвидеть возможность наступления тяжких последствий[32].

Так, приговором Коминтерновского районного суда г. Воронежа от 24.04.2017 по делу № 1-271/2017 было установлено, что члены организованной группы, осознавая общественную опасность своих действий и наступление последствий, распределив между собой преступные роли, лицо №1, лицо №2, лицо №4, лицо №3, (ФИО6), (ФИО26), лицо №7, лицо №6, лицо №5 и Рыжов А.Н. преступили к стадии подготовки технических и программных средств, необходимых для внедрения в сеть автозаправочных комплексов

[32] Галкин А.И. Уголовная ответственность за преступления в сфере компьютерной информации // Следователь. Федеральное издание. - М., 2009, № 5 (133). - С. 7.

ОАО «Воронежнефтепродукт» вредоносного программного обеспечения. С этой целью лицо №6, действуя в соответствии с отведенной ему ролью, являясь программистом, находясь в «адрес» и осуществляя взаимодействие через лицо №5, на основе имеющихся заготовок, используя язык программирования «С++» в среде разработки фирмы «Borland (Embarcadero)» с применением технического средства-ноутбука «Panasonic CF-19» создало и предоставило последнему необходимый комплект исходных текстов модифицированного микропрограммного кода для электронных блоков «Калькулятор Т-20» и «Диалоговый модуль» ТРК марки «Scheidt&Bachmann», содержащего не предусмотренные заводом изготовителем функции недолива нефтепродуктов, а также корректировки суммарных счетчиков ТРК. Помимо этого, лицо №6 предоставило лицу №5 исходные тексты компьютерных программ, предназначенные для удаленного управления вышеуказанными функциями по сети LON (Local Operating Networks).

В июле 2012 года лицо №5, Рыжов А.Н. прибыли на АЗК №71 ОАО «Воронежнефтепродукт», расположенному по адресу: «адрес», где в присутствии (ФИО25) произвели успешное тестирование работоспособности вредоносного программного обеспечения.

Летом 2012 года лицо №7, действуя в соответствии с отведенной ему ролью, находясь в «адрес», используя язык программирования «С++», создало исходный текст компьютерной программы, с помощью которого стало возможным осуществлять компиляцию вредоносной компьютерной программы, предназначенной для стирания в базе данных АСУ «Сибинтек АЗС» сведений о технологических проливах, о чем сообщило лицу №4.

Далее, летом 2012 года лицо №1, лицо №2, лицо №4, лицо №3, (ФИО6), (ФИО26), лицо №7, лицо №6, лицо №5 и Рыжов А.Н. понимая, что все необходимые программные и технические средства для перепрограммирования ТРК протестированы и готовы для планомерного внедрения в сеть АЗК ОАО «Воронежнефтепродукт», действуя каждый в соответствии с отведенной ему преступной ролью, используя персонал АЗК ОАО «Воронеж-

нефтепродукт», в период с 07.07.2012 г. по 26.07.2014 г., используя для обмена данными криптографические средства шифрования информации, осуществили распространение и использование вредоносного программного обеспечения на 27 АЗК ОАО «Воронежнефтепродукт».

2.4. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ)

Часть 1 статьи 274 Уголовного кодекса гласит, нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб, наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев 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.

По части 2 статьи 274 Уголовного кодекса рассматривается деяние, предусмотренное частью первой настоящей статьи, если оно повлекло тяжкие последствия или создало угрозу их наступления и наказывается принудительными работами на срок до пяти лет либо лишением свободы на тот же срок.

Статья 274 Уголовного кодекса устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, акцентируя, что оно, это деяние, должно причинить существенный вред. Нацелена данная статья на предупреждение невыполнения пользователями

своих профессиональных обязанностей, влияющих на сохранность хранимой и передаваемой информации. Эта уголовная норма отсылает к ведомственным правилам и инструкциям, определяющим порядок работы, которые должны устанавливаться специально уполномоченным лицом и доводиться до пользователей.

Действие данной статьи распространяется только на компьютеры и локальные сети организаций и не применимо для публичного доступа, например, глобальной сети Интернет.

Непосредственный объект преступления, предусмотренный статьей 274 УК – определённые отношения по исполнению правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Дополнительным объектом, как правило, может выступать авторское право, право собственности, право на неприкосновенность частной личной жизни, и семейную тайну и др.

Объективная сторона - нарушение правил эксплуатации. Под такими правилами понимаются: гигиенические требования по уходу за компьютерной техникой, наличие и хранение технической документации на приобретаемые компьютерные средства и конкретные, и другие правила доведенные под роспись до работников.

Еще одним признаком объективной стороны состава преступления, предусмотренного ст. 274 УК РФ являются последствия вредоносного характера. Законодатель их предусмотрел в виде блокирования, модификации, уничтожения, или копирования информации, если это деяние повлекло причинение крупного ущерба.

Часть 2 ст. 274 Уголовного кодекса предусматривает ответственность за деяния, повлекшие тяжкие последствия, или создавшие угрозу их наступления. Под тяжкими последствиями нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей понимается окончательная утрата осо-

бо ценной информации, поломки важных технических средств (в том числе авианавигационной техники и оборонного значения), повлекшие катастрофы, аварии, гибель людей. При этом необходимо иметь в виду, что наступившие последствия могут квалифицироваться в совокупности с другими преступлениями в зависимости от их характера и отнесения заведомо к легкомыслию или к косвенному умыслу в виде безразличного отношения к последствиям.

Субъект данного преступления - специальный.

Субъективная сторона преступления, предусмотренного ч.1 ст. 274 УК РФ это вина в виде прямого или косвенного умысла. Преступление, предусмотренное ч. 2 ст. 274 УК РФ, совершается с «двойной» формой вины: умышленной по отношению к нарушению правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, неосторожной по отношению к наступившим тяжким последствиям, так как нарушая установленные правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, должностное лицо не рассчитывает на умысел в наступлении тяжких последствий.

2.5. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1. УК РФ)

Часть 1 статьи 274.1 Уголовного кодекса гласит, что создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации наказуемо принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от

пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Часть 2 статьи 274.1 Уголовного кодекса гласит, что неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации наказуемо принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осужденного за период от одного года до трех лет.

Часть 3 статьи 274.1 Уголовного кодекса гласит, что нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации наказуемо 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 шести лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

В связи с принятием Федерального закона от 26.07.2017 N 187-ФЗ “О безопасности критической информационной инфраструктуры Российской Федерации”, в Уголовный кодекс Российской Федерации, Федеральным законом от 26.07.2017 N 194-ФЗ “О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации” введена статья 274.1. УК РФ, которая вступила в силу с 01.01.2018 г. Основной причиной появления данной статьи в УК РФ является необходимость борьбы с компьютерными атаками на информационные ресурсы Российской Федерации, то есть обеспечение безопасности объектов критической информационной инфраструктуры. В связи с этим появляется ряд вопросов о модернизации законодательной техники при конструировании данной статьи, регламентации уголовной ответственности при совершении преступления в этой сфере. Состав преступления, предусмотренный ст. 274.1 УК РФ, специальный заключается в специфике закрепленного в нем предмета преступления.

Предмет преступления - компьютерная информация, содержащаяся в критической информационной инфраструктуре Российской Федерации, либо сама критическая информационная инфраструктура РФ. Таким образом, диспозиция ст. 274.1 УК РФ для определения признаков преступления отсылает нас к специальным нормативно-правовым актам. Для этого необходимо ссылаться на вышеупомянутый Федеральный закон “О безопасности критической информационной инфраструктуры Российской Федерации” и установить особые признаки. Взаимодействие информационной инфраструктуры, использование автоматизированные системы управления, информационные системы государственным учреждениям, российским юридическим лицам и (или) индивидуальным предпринимателям в сфере здравоохранения, транспорта, науки, энергетики, связи, банковской сфере и иным сферам финансо-

вого рынка, к области атомной энергии, топливно-энергетического комплекса, оборонной, горнодобывающей, ракетно-космической, химической и металлургической промышленности. Должны быть значимыми, включены в реестр значимых объектов критической информационной инфраструктуры и им должна быть присвоена одна из категорий значимости (первая, вторая или третья). Должны находиться на территории РФ в дипломатических представительствах и (или) консульских учреждениях РФ и относиться к информационным ресурсам РФ.

Таким образом, вышеназванные признаки необходимы для определения предмета преступления, предусмотренного ст. 274.1 УК РФ и должны устанавливаться в совокупности. При этом их можно считать по большей мере оценочными и учитывать в каждом конкретном случае следствием и судом.

К примеру, в процессе квалификации преступления по ст. 274.1 УК РФ произошло изменение категории значимости объект критической информационной инфраструктуры в порядке, предусмотренном для категорирования. В связи с чем, предмет рассматриваемого преступления утратил свои признаки и необходима переквалификация установленного деяния по иным статьям главы 28 УК РФ о преступлениях в сфере компьютерной информации. К сожалению, этот процесс возможен на любых этапах уголовно-правовых отношений: от привлечения к уголовной ответственности до снятия либо погашения судимости. Тем более, что исходя из положений п. 12 ст. 7 закона “О безопасности критической информационной инфраструктуры РФ”, не указано, как может быть изменена категория значимости объектов – в сторону повышения или снижения значимости. И нет никаких препятствий повторять этот процесс изменения значимости несколько раз.

Изначально ст. 274.1 УК РФ введена в главу 28 с целью предусмотрения ответственности за деяния, обладающие повышенной общественной опасностью по сравнению с деяниями, отраженными в ст. 272-274 УК РФ и затрагивающими государственные интересы. И эта разница в общественной

опасности должна была найти свое отражение в первую очередь в жесткости санкций указанных составов.

Но при сравнении санкций общих и специального состава, эта разница в общественной опасности прослеживается не достаточно четко. Это касается сравнения ч. 1 ст. 273 УК РФ и ч. 1 ст. 274.1 УК РФ – оба преступления средней тяжести, и санкция вновь вводимого состава позволяет судам назначать наказание меньшее, чем пять лет лишения свободы (от двух до пяти).

Отсутствие нижнего предела размера наказания предусмотренного ч. 3 ст. 274.1 УК РФ - лишение свободы сроком до шести лет, является недостатком, позволяющим сопоставить данную часть с ч. 1 ст. 274 УК РФ, так как у судов есть возможность назначать наказание в виде лишения свободы сроком на два года. И тогда исчезает грань в оценке уровня общественной опасности при квалификации деяния, как по общему, так и специальному составу преступления против компьютерной информации.

Аналогичная ситуация складывается (суд может назначить равные сроки наказания в виде лишения свободы) и при назначении наказания за данные преступления, совершенные групповым способом (за преступления, предусмотренные ч. 4 ст. 274.1 УК РФ и ч. 3 ст. 272, ч. 2 ст. 273 УК РФ).

Учитывая, что рассматриваемая статья в УК РФ достаточно новая по сравнению с точкой отсчета появления в свет 28 главы, а приступные посягательства и различного рода кибер атаки на критическую информационную инфраструктуру набирают свои обороты и во многом приобретают политический характер, законодателю предстоит еще много вносить поправок в ее содержание.

ГЛАВА 3. ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

3.1. Значение термина «компьютерная информация» для квалификации компьютерных преступлений

Широкое внедрение информационных технологий и приводимая многими авторами статистика свидетельствует о том, что вопросы квалификации преступлений, предусмотренных главой 28 УК РФ, продолжают оставаться актуальными. С момента появления первых сообщений о преступной активности в компьютерной сфере специалистами отмечается особая опасность[33] и широкий спектр[34] преступлений, направленных против компьютерной информации. Другими особенностями компьютерной преступности, которые требуют особого внимания, по мнению специалистов, является их прогрессирующий количественный рост. Все эти негативные аспекты сопровождаются фактором высокой латентности, которая по разным экспертным оценкам, достигает показателей от 90%[35] до 99,8%[36].

Одной из причин такого положения является терминологическая неопределенность, по сравнению с другими видами преступлений. Наибольший разброс мнений наблюдается в определении понятия «компьютерная информация», тогда как этот термин является ключевым для понимания всех составов главы 28 УК РФ. Специалисты различных направлений под компьютерной информацией понимают: «Информацию, размещенную на машинном носителе, в электронно-вычислительной машине «ЭВМ», системе ЭВМ или их сети»[37]; «фактические данные, обработанные компьютером полученные на его выходе в форме, доступной восприятию человеком либо ЭВМ или пере-

[33] Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Волгоград, 1998. С.4.
[34] Остроушенко А.В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации: автореф. дис. канд.юрид. наук. Волгоград, 2000, С. 4.
[35] Вехов Б.В. Компьютерные преступления: способы совершения, методика расследования. М., 1996. С. 44; Федоров В.И. Борьба с транснациональной организованной преступностью в сфере «высоких технологий» // прокурорская и следственная практика. 1999. №3. С.31.
[36] Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. канд.юрид. наук. Иркутск, 2006. С.19.
[37] Егорышев А.С. Расследование и предупреждение неправомерного доступа к компьютерной информации: автореф. дис. канд. юрид. наук. Самара, 2004. С.10.

сылающиеся по телекоммуникационным каналам»[38]; «информацию, предоставленную в специальном (машинном) виде, пригодном и предназначенном для ее автоматизированной обработки, хранения и передачи, находящуюся на материальном носителе и имеющую собственника или иного законного владельца, установившего порядок ее создания, обработки, передачи и уничтожения»[39]. Имеются также мнения, что информация и сведения тождественны, а информация и сообщения - синонимы.

Понимание информации в российской правовой традиции традиционно ассоциировалось с документом[40]. В современной России Стрельцов А.А., обосновал информацию как результат отражений объектов материального мира в виде сведений и сообщений[41].

Теоретические разработки отечественных и зарубежных ученых на этом не исчерпываются, но для понимания природы компьютерной информации выделены основные составляющие: значение (смысл, содержание) и сигнал. Смысл – это та часть, которая аналогична смыслу, переданному документом. Для понимания компьютерного сигнала необходимо определить, что именовать компьютером – источником сигнала. В цепи человек-получатель информации (значения, смысла) – источник информации компьютер является промежуточным звеном. Это технико-технологическое устройство может обладать свойствами, качествами, которые активно способствуют либо препятствуют информационному процессу.

По мнению Черняка Л., слово компьютер происходит от латинского computare (com- вместе, putare- считать). Оно обозначало специфические расчеты, связанные с определением даты Пасхи; параллельно для простых вычислений существовало слово calculus (исчисление)[42]. Современные пред-

[38] Мусаева У.В. Розыскная деятельность следователя по делам о преступлениях в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Тула. 2002. С. 18

[39] Мещаряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Воронеж, 2001, С. 14-15.

[40] Гаврилов О.А. Курс правовой информатики. М., 2000; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право /под ред. Б.Н. Топорнина. Спб., 2001.

[41] Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы /под ред. В.А. Садовнического, В.П. Шерстюка. М., 2002. С. 23-37.

[42] Черняк Л. Это древнее слово «компьютер» // Computerworld. 2005. №10(459). С.36.

ставления об электронных вычислительных машинах, особенно о наиболее распространенной категории, именуемой персональные компьютеры или компьютеры, в целом соответствует их функциональному назначению – сложные вычисления. Тем не менее, в литературе встречаются мнения о существовании «электронных устройств, которые нельзя отнести к классу ЭВМ (некоторые сложные калькуляторы, игровые приставки, мобильные телефоны сотовой связи, способные не только обеспечивать телефонную связь, но и снабжены большим количеством дополнительных функций (смартфоны))»[43]. Существуют утверждения о необходимости введения «единого понятия компьютерного объекта».

Таким образом, на практике термин «компьютерная информация» может весьма сильно отличаться в зависимости от того, кто и как его понимает. Существующая неопределенность в понимании компьютерной информации должна быть преодолена на основе междисциплинарных и межотраслевых исследований. Естественное технологическое развитие информационной среды и соответствующее проникновение во все сферы жизни компьютеров также должны стать объектом внимания уголовного права, в целях точного определения пределов криминализации деяний, связанных с понятием «компьютерная информация»[44].

3.2. Актуальные проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации

Совершение преступлений в виде неправомерного доступа к компьютерной информации, создания, использования и распространения вредоносных программ зачастую является одним из этапов совершения других преступлений, которые не входят в состав 28 главы УК РФ и по своим признакам не имеют никакого отношения к охране компьютерной информации, та-

[43] Хатунцев Н.А. Теоретические и методические основы судебной компьютерно - технической экспертизы при разрешении споров хозяйствующих субъектов: автореф. дис. к.ю.н. М., 2006. С.14.
[44] Волков Ю.В. Значение термина компьютерная информация // Уголовное право: стратегия развития в XXI веке. Материалы 6-й международной научно-практической конференции 29-30 января 2009г.. –М.: проспект, 2009. С.415-518.

кие как вымогательство, мошенничество и т.д. В связи с этим внимание уделяется вопросам квалификации преступлений в сфере компьютерной информации по совокупности с другими преступлениями и на вопросах их отграничения от таких преступлений.

Так, Степанов А.Б. совершил неправомерный доступ к охраняемой законом компьютерной информации, что повлекло блокирование, модификацию и копирование компьютерной информации; кроме того он нарушил тайну переписки; а также совершил вымогательство , то есть требование передачи чужого имущества под угрозой распространения сведений, которые могли причинить существенный вред законным интересам потерпевшего, данные преступления были совершены им в г.Новосибирске, при следующих обстоятельствах:

Эпизод №1:

У Степанова А.Б. возник преступный умысел на неправомерный (несанкционированный правообладателем) доступ к охраняемой законом информации о фактах, событиях и обстоятельствах частной жизни, принадлежащей ФИО1, расположенной в электронном ящике электронной почты ..., программы ..., на странице ФИО1 социальных сетей ... Интернет-ресурса ... и ... электронный адрес ..., после чего реализуя данные преступные намерения, направленные на неправомерный доступ к компьютерной информации о ранее знакомой ему ФИО1, Степанов А.Б., находясь по месту своего жительства, используя принадлежащий ему ноутбук, подключенный к глобальной сети «Интернет», заведомо зная о порядке и правилах осуществления выхода в сеть Интернет, действуя умышленно, с целью незаконного получения пароля доступа, зашёл на ящик электронной почты, где обратился к ссылке «Забыли пароль», после чего, действуя по указаниям провайдера социальных сетей, с целью восстановления пароля, выбрал ссылку «Ответ на секретный вопрос», после чего ему было предложено ответить на вопрос «На какой улице родилась?», ответ на который Степанову А.Б. был известен из общения с ФИО1, после ответа на поставленный вопрос Степанову А.Б. был выслан но-

вый пароль для входа на ящик электронной почты, после чего Степанов А.Б. получил возможность незаконного доступа к информации, хранящейся в указанном электронном ящике электронной почты и доступа на интернет-страницу ФИО1, тем самым Степанов А.Б. совершил неправомерный (несанкционированный правообладателем) доступ к охраняемой законом информации о фактах, событиях и обстоятельствах частной жизни, принадлежащей абоненту ФИО1.

После этого, Степанов А.Б. действуя умышленно, заменил пароль доступа к электронному ящику электронной почты и доступ пароля к электронному адресу, тем самым модифицировал информацию, заблокировав доступ законного обладателя ФИО1 к охраняемой законом компьютерной информации об обстоятельствах частной жизни, расположенной в электронном ящике электронной почты, принадлежащий ФИО1 и на странице ФИО1 социальной сети, лишив ФИО1 возможности пользоваться ими, после чего, Степанов А.Б., действуя в продолжение своих преступных намерений, направленных на неправомерный доступ к охраняемой законом компьютерной информации о фактах, событиях и обстоятельствах частной жизни ФИО1, действуя умышленно, незаконно скопировал информацию с интернет-страницы социальной сети ФИО1 в виде переписки ФИО1 с ФИО2 и переместил файл с перепиской к себе на ноутбук.

Эпизод №2:

У Степанова А.Б. возник преступный умысел, направленный на нарушение тайны переписки, охраняемой ст.23 Конституции РФ, расположенной в электронном ящике электронной почты ... программы ..., социальных сетей ... Интернет-ресурса ... и Интернет-ресурса ... электронный адрес ..., пользователем которых являлась ФИО1 и вела электронную переписку с ФИО2, реализуя который, Степанов А.Б., действуя умышленно, заведомо зная о порядке и правилах осуществления выхода в сеть Интернет, зная пароли входа на интернет-ресурсы, которые были получены им незаконным путём, находясь по месту своего жительства, используя принадлежащий ему ноутбук,

подключенный к глобальной сети Интернет, желая ознакомиться с ее информацией, незаконно зашёл в социальную сеть ..., пользователем которого являлась его знакомая ФИО1, где незаконно ознакомился с перепиской ФИО2, адресованной ФИО1, содержащей сведения интимного характера об их частной жизни, тем самым Степанов А.Б., действуя умышленно, нарушил тайну переписки, охраняемую ст.23 Конституции РФ.

Эпизод №3:

У Степанова А.Б. возник преступный умысел, направленный на незаконное требование передачи чужого имущества под угрозой распространения сведений, скаченных им через Интернет, которые могли нанести законным интересам ФИО2 существенный вред, выразившийся в распаде семьи последнего, реализуя который, Степанов А.Б. в неустановленном месте и в неустановленное время, располагая сведениями об интимных отношениях между ФИО2 и ФИО1, полученных им ранее незаконным путём в сети Интернет в результате взлома пароля доступа на интернет-страницу ..., пользователем которой являлась ФИО1, имея преступный умысел на хищение имущества ФИО2, под угрозой распространения сведений интимного характера его супруге, действуя умышленно, позвонил последнему по телефону и незаконно потребовал от ФИО2 передачи ему денежных средств в сумме 80.000 рублей, при этом в случае отказа высказал угрозу предоставить супруге ФИО2 электронную переписку с ФИО1 Далее, Степанов А.Б., действуя в продолжение своих преступных намерений, направленных на незаконное требование передачи ему чужого имущества под угрозой распространения сведений, которые могли причинить существенный вред законным интересам ФИО2, выразившийся в разводе супругов, неоднократно осуществлял телефонные звонки со своего телефона на телефон ФИО2, продолжая вымогать деньги у ФИО2 под угрозой распространения сведений об интимных отношениях последнего с ФИО1, при этом в случае невыполнения его требований о передаче ему денежных средств в сумме 90.000 рублей, угрожал предоста-

вить в подтверждение супруге ФИО2 интернет-переписку между ФИО1 и ФИО2, что привело бы к разводу супругов.

Далее, Степанов А.Б., в подтверждение своих намерений, доказывая наличие у него компрометирующей информации на ФИО2, переслал последнему по электронной почте интернет-переписку между ФИО1 и ФИО2, содержащую сведения интимного характера, которая была получена Степановым А.Б. незаконным путём, а также Степанов А.Б., действуя в продолжение своих противоправных действий, со своего телефона неоднократно отправлял смс-сообщения на телефон ФИО2, в которых выражались незаконные требования о передаче денежных средств за нераспространение сведений супруге ФИО2 об интимной связи последнего с ФИО1. Кроме того, действуя во исполнение задуманного, Степанов А.Б., действуя умышленно, с целью незаконного получения денежных средств за нераспространение сведений интимного характера, которые могли причинить существенный вред законным интересам ФИО2, а именно развод с женой, назначил ФИО2 встречу возле здания отдела полиции №5 «Дзержинский» Управления МВД России по г.Новосибирску, после чего, в ходе данной встречи, Степанов А.Б., реализуя свои преступные намерения, направленные на незаконное требование передачи чужого имущества под угрозой распространения сведений супруге ФИО2 об его интимной связи с ФИО1, действуя умышленно, получил от ФИО2 10.000 рублей, ранее врученные ФИО2 для проведения оперативно-розыскного мероприятия, а затем Степанов А.Б., действуя в продолжение своих противоправных действий, направленных на незаконное получение денежных средств за нераспространение сведений интимного характера, которые могли причинить существенный вред законным интересам ФИО2, а именно развод с женой, назначил ФИО2 встречу в кафе «Н», где в ходе встречи Степанов А.Б., реализуя свой преступный умысел на вымогательство денежных средств под угрозой распространения сведений об измене ФИО2 его супруге, действуя умышленно, получил от последнего за неразглашение имеющейся информации денежные средства в сумме 10.000 рублей, после

чего был задержан сотрудниками полиции и в ходе личного досмотра у Степанова А.Б. были обнаружены и изъяты денежные средства в сумме 10.000 рублей, ранее врученные ФИО2 для проведения оперативно-розыскного мероприятия «оперативный эксперимент», тем самым, Степанов А.Б. незаконно получил денежные средства в сумме 20.000 рублей, переданные ФИО2 по требованию Степанова А.Б. за нераспространение сведений об интимных отношениях между ФИО1 и ФИО2 супруге последнего.

Суд квалифицировал действия Степанова А.Б. по эпизоду №1 приговора - по ч.1 ст.272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, повлекший блокирование, модификацию и копирование компьютерной информации; по эпизоду №2 приговора - по ч.1 ст.138 УК РФ – нарушение тайны переписки; а по эпизоду №3 приговора - по ч.1 ст.163 УК РФ – вымогательство, то есть требование передачи чужого имущества под угрозой распространения сведений, которые могли причинить существенный вред законным интересам потерпевшего.

Преступления в сфере компьютерной информации как правило совершаются в совокупности с иными общественно опасными деяниями и имеют факультативный характер. Встретить их в обособленном виде большая редкость[45].

«Электронная цифровая подпись» посредством специальной программы обеспечивает идентификацию компьютерной информации, т.е. подтверждает факт «подписания» ее конкретным лицом, оригинальность содержащихся в ней сведений, реквизитов документа[46].

Если рассматривать статью 272 УК РФ, то можно установить, что не каждый случай неправомерного доступа к компьютерной информации подпадает под ее действие.

[45] Костин В.П. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики: автореф. дисс. к.ю.н. Н. Новгород, 2007. С.6.

[46] Айсанов Р.М. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ //»Черные дыры» в Российском Законодательстве. Юридический журнал. – М.: «1К-Пресс», 2006, №3. С. 140.

Так, приговором суда было установлено, что у Овчинникова С.О., имевшего при себе пластиковую банковскую карту «Maestro» Сбербанка России, оформленную на Потерпевшего № 1, которую в один из дней начала апреля 2016 года Потерпевший № 1 добровольно передал Овчинникову С.О. во временное пользование, сказав при этом «пин - код» от данной банковской карты, возник преступный умысел на совершение тайного хищения денежных средств с лицевого счета Потерпевшего №1 вышеуказанной банковской карты.

Реализуя свой преступный умысел, направленный на тайное хищение денежных средств, принадлежащих Потерпевшему № 1 с банковской карты «Maestro» Сбербанка России, Овчинников С.О. в вышеуказанный период времени, действуя умышленно из корыстных побуждений, с целью тайного хищения чужого имущества, с целью извлечения имущественной выгоды, путем свободного доступа , осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно-опасных последствий в виде причинения значительного материального ущерба Потерпевшему №1 и желая их наступления, решил, предварительно завладеть персональными средствами доступа к системе «Сбербанк онлайн» (идентификатор, постоянный и одноразовые пароли), с помощью системы «Сбербанк онлайн» и осуществлять операции по переводу денежных средств со счета банковской карты «Maestro» Сбербанка России, оформленной на Потерпевшего №1, тем самым похитить денежные средства Потерпевшего №1, находящиеся на его лицевом счете банковской карты.

После чего, Овчинников С.О., находясь в помещении, где расположен банкомат Сбербанка России, без ведома Потерпевшего №1, с помощью банкомата подключил к банковской карте «Maestro» Сбербанка России, оформленной на Потерпевшего №1, банковские услуги «Мобильный банк» и «Сбербанк онлайн» к сотовому телефону с абонентским номером, находящегося в пользовании Р. Таким образом, Овчинников С.О. получил идентификатор, постоянный и одноразовые пароли к персональным средствам доступа

к системе «Сбербанк онлайн» по банковской карте Потерпевшего №1 с целью последующего контроля баланса банковской карты последнего и перевода с его банковской карты денежных средств, при этом Овчинников С.О. переписал идентификатор и постоянный пароль на обложку тетради и оставил ее себе.

Далее, Овчинников С.О. с помощью находящегося у него нетбука, подключенного к сети «Интернет», зашел в систему «Сбербанк онлайн», подключенной к вышеуказанной банковской карте Потерпевшего №1, где с помощью находящегося у него ранее полученного идентификатора и постоянного пароля, осуществил доступ к личному кабинету системы «Сбербанк онлайн» Потерпевшего №1, содержащему сведения о его банковских счетах (картах), остатках денежных средств на счете и проверил баланс банковской карты Потерпевшего №1, на балансе банковской карты которого находились денежные средства в сумме 8471 руб. 80 коп. После этого Овчинников С.О. перевел в системе «Сбербанк онлайн» с лицевого счета банковской карты Maestro» Сбербанка России, оформленной на Потерпевшего №1, на лицевой счет своей банковской карты «Maestro» Сбербанка России денежные средства в сумме 8400 руб., принадлежащие последнему.

Далее, Овчинников С.О., находясь в помещении, где расположен банкомат Сбербанка России, обналичил со своей банковской карты «Maestro» Сбербанка России денежные средства в сумме 8400 руб., которые ранее перевел с лицевого счета Потерпевшего №1 вышеуказанной банковской карты.

В судебном заседании государственный обвинитель просил исключить из предъявленного Овчинникову С.О. обвинения, как излишне вмененные ч. 3 ст. 183 УК РФ, ч. 2 ст. 272 УК РФ, поскольку согласно материалам уголовного дела, умысел подсудимого был направлен на хищение денежных средств потерпевшего и получение сведений о пароле от системы автоматизированного облуживания клиентов «Сбербанк онлайн», доступ к указанной системе, являются способом совершения преступления.

Суд, соглашаясь с мнением государственного обвинителя, исключает из обвинения, предъявленного Овчинникову С.О., как излишне вмененные ч. 3 ст. 183 УК РФ, ч. 2 ст. 272 УК РФ.

Приговор Козельского районного суда Калужской области от 08.05.2018 по делу № 1-1-57/2018.

Кроме того, нельзя считать полным перечень общественно опасных последствий, указанных в диспозиции ст. 272 УК РФ, так как даже простое ознакомление с компьютерной информацией (не указанное в ст. 272 УК РФ) в результате незаконного доступа может нанести неисправимый ущерб собственнику информации. Указанная точка зрения оспаривается рядом авторов[47].

Способы неправомерного доступа к компьютерной информации бывают самыми различными, например: изменение кода или адреса технического устройства, представление поддельных документов на право доступа к информации, повреждение средств или системы защиты информации, кража носителя информации[48]. В случае неправомерного завладения компьютерным устройством как вещью без электропитания или электронным носителем информации (например похищение флэш карты), не рассматривается как доступ к компьютерной информации и в соответствующих случаях может повлечь ответственность по статьям о преступлениях против собственника или самоуправстве.

В данном случае необходимо тщательно анализировать какими мотивами и целями руководствовался преступник, на что был направлен умысел.[49].

---

[47] Комментарий к УК РФ с постатейными материалами и судебной практикой / под ред. д.ю.н., проф. Улезько С.И. Ростов н/Д., 2002. С. 676 (автор главы - к.ю.н. Воронцов С.А.); Комментарий к Уголовному кодексу РФ / под ред. д.ю.н. проф. А.Г. Королькова. М.; 2004. С.798 (авторы главы - Ю.В. Белянинова, А.М. Дедов); Комментарий к Уголовному кодексу Российской Федерации / под ред. В.И. Радченко, А.С. Михлина. Спб., 2008. С.566 (автор главы - д.ю.н., проф. А.Н. Попов).

[48] Коммернтарий к УК РФ / отв. ред. д.ю.н. А.В. Наумов. М., 1996. С.664 (автор главы – д.ю.н., профессор С.В. Бородин).

[49] Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дис. к.ю.н. Красноярск, 2002. С. 145.

Поскольку физические лица инфрмация считают собственностью , целесообразно включить в квалифицированный состав ст. 272, 273 УК РФ еще один объект – отношения собственности.

В настоящее время при отсутствии судебной практики Верховного Суда РФ по вопросам, связанным с причинением ущерба компьютерными преступлениями, можно было бы использовать практику расчета ущерба при нарушении авторских и смежных прав, так как, согласно ч. 1 ст. 1259 ГК РФ, к объектам авторских прав также относятся программы, которые охраняются как литературные произведения[50].

С 01.01.2018 г. в 28 главу УК РФ введена статья, предусматривающая ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. До этого момента на протяжении долгих лет она оставалась неизменной, не взирая на то, что ответственность за преступления против компьютерной информации или за преступления, совершенные при помощи компьютерной информации является все более актуальным в науке уголовного права и нуждается в дальнейшем обновлении.

Учитывая, что интернет не имеет границ, будет логичным дополнить объективную сторону преступления, предусмотренного ст. 272, 273, ст. 274.1 УК РФ, новыми квалифицирующими признаками: «… то же деяние, совершенное на территории Российской Федерации в отношении, охраняемой законом информации, находящейся за пределами Российской Федерации, - …», и «то же деяние, совершенное за пределами Российской Федерации в отношении охраняемой законом информации на территории Российской Федерации. - …», что позволит учесть международный аспект преступления. Тем самым Россия сможет привести свое уголовное законодательство в соответ-

[50] «Гражданский кодекс Российской Федерации (часть четвертая)» от 18.12.2006 №230-ФЗ (ред. от 23.05.2018).

ствие с принятыми на себя международными обязательствами в борьбе с преступлениями в сфере компьютерной информации[51].

[51] Ст. 2 Соглашения о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (подписано 01.06.2001 в Минске); окинавская хартия глобального информационного общества (принята 22.07.200 г. на Окинаве (Япония) на совещании руководителей глав государств и правительств стран «Группы Восьми»).

ЗАКЛЮЧЕНИЕ

В данной выпускной квалификационной работе наиболее подробно охвачена тема компьютерных преступлений и освящены наиболее часто возникающие вопросы при их квалификации и применении в действующем законодательстве. Из всего вышеизложенного можно сделать главный вывод о том, что глава 28 Уголовного кодекса Российской Федерации имеет большие правовые пробелы, в связи, с чем и появляются проблемы при квалификации компьютерных преступлений и смежных с ней сферах.

Данная тема является актуальной, так как сегодня можно с уверенностью говорить о переходе общества в новую, информационную фазу развития, для которой характерно формирование новой идеологии, новых социальных слоев со своей особой культурой, психологией, системой ценностных ориентаций, интересами и потребностями. На этом фоне возникли и активно развиваются информационные отношения.

Определяющей чертой информационного общества является то, что информация, информационные ресурсы, средства и методы их создания, хранения, обработки, передачи и потребления составляют неотъемлемую часть механизма функционирования всех основных сфер социально-политической жизни, оказывают на них определяющее влияние. Процесс создания условий, необходимых для обеспечения информационных и иных потребностей и реализации прав общественных объединений, государственных органов, граждан, на основе формирования и использования информационных ресурсов, называется внедрением информационных технологий.

Формирование информационного общества обусловлено и одновременно порождает возникновение и интенсивное развитие информационной сферы, в которой информация предоставляет не только в традиционном качестве знаний, сведений, но и в качестве товара, оружия, услуг, ресурсов. Уникальные свойства информационной сферы могут быть использованы и используются как на благо, так и во вред обществу. Информация создает условия и

предпосылки трансформации существующих и возникновения качественно новых видов угроз интересам личности, общества, государства. Причем угроз, как в самой информационной сфере, так и в иных сферах социально-политической жизни, неразрывно связанных с последней.

Внедрение информационных технологий несет широкое и повсеместное распространение компьютеров, цифровых технологий. Это определяет новые возможности, интересы и потребности личности, общества и государства в информационной и смежной с ней сферах и одновременно порождает новые угрозы этим интересам. Все эти интересы реализуются в рамках и посредством участия субъектов социально-политической жизни в информационных отношениях.

Осознание социально-политической значимости информационных отношений - отношений, возникающих в связи и по поводу реализации субъектами своих частных и общих интересов в информационной и смежной с ней сферах требует совершенствования их нормативно-правовой регламентации, повышения эффективности юридических средств и методов реализации информационного права и формирования адекватных юридических механизмов защиты интересов субъектов информационных правоотношений, прежде всего, путем совершенствования механизма реализации уголовной ответственности, наступающей за совершение преступных деяний в сфере компьютерной информации.

По моему мнению, необходимо рассматривать преступную деятельность в сфере компьютерной информации как источник угроз информационной и, в целом, национальной безопасности Российской Федерации, а преступления в сфере компьютерной информации – как реальные угрозы жизненно важным интересам личности, общества и государства во всех сферах их жизнедеятельности.

В данной работе затронута и изучена уголовная ответственность за преступления в сфере компьютерной информации за границей, так как для эффективной борьбы с преступлениями в данной сфере необходимо учитывать

опыт борьбы других стран. В последнее время масса правонарушений в области компьютерных технологий увеличивается, поэтому все заинтересованные страны должны объединить свои усилия в борьбе с ними. Проблема противодействия данных преступлений не может быть решена в отдельном взятом государстве, потому что кибер преступления распространились по всему миру. Необходимо развивать сотрудничество, обмен опытом, международное право в данной области, также создавать единое правовое поле для решения проблем борьбы с преступлениями в сфере информационных технологий.

Уголовное законодательство Российской Федерации содержит в себе нормы нацеленные на защиту компьютерной информации. Необходимость формирования уголовной ответственности за причинение вреда в связи с использованием компьютерной информации (т.е. информации на машинном носителе) вызвана постоянно развивающимся рынком цифровых технологий, а вместе с тем, в связи с их применением во многих сферах деятельности, повышением уязвимости компьютерной информации по сравнению, с информацией, зафиксированной на бумаге и хранящейся в трудно доступном месте.

Анализ статей 272, 273, 274, 274.1 УК РФ показывает, что именно копирование, модификация, блокирование и уничтожение – все эти свойства охраняются главой 28 УК РФ.

По моему мнению, такое действие, как «ознакомление» может нанести существенный вред владельцу информации. Поэтому, анализируя все выше сказанное, для более точной квалификации данного преступления я считаю, что необходимо внести изменения в ч. 1 ст. 272 и изложить ее в следующей редакции:

1. Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло несанкционированное ознакомление, уничтожение, блокирование, модификацию либо копирование компьютерной информации.

Так же в ч. 4 ст. 272 УК устанавливается, что деяния, предусмотренные частями первой, второй или третьей настоящей статьи, если они по-

влекли тяжкие последствия или создали угрозу их наступления, наказываются лишением свободы на срок до семи лет. Однако законодатель не раскрывает понятие, о каких тяжких последствиях идет речь, что затрудняет применение данной нормы.

2. Нудно включить в состав ч. 2 ст. 272 УК РФ отношения собственности, тем самым признав потерпевшего обязательным признаком объекта состава преступления и дополнив ст. 272 УК РФ новым квалифицирующим признаком "с причинением значительного ущерба гражданину..."

Все эти факторы доказывают еще раз, что глава 28 УК РФ требует весомых доработок и изменений.

Преступления в сфере компьютерной информации, предусмотренные Уголовным кодексом РФ в главе 28 на сегодняшний день являются одними из наиопаснейших преступлений нового типа. В связи с постоянно развивающимся рынком цифровых технологий для правильной, соразмерной и более точной квалификации данных деяний необходимо в ногу со временем анализировать, прогнозировать и вносить изменения в статьи указанной главы Уголовного кодекса. Это положительно отразится на борьбе с данными видами преступлений и приведет к более качественной защите электронной информации и безопасности.

СПИСОК ИСТОЧНИКОВ

Нормативно-правовые акты

1. "Гражданский Кодекс Российской Федерации (часть первая)" от 30.11.1994 N 51-ФЗ (ред. от 03.08.2018).
2. "Гражданский Кодекс Российской Федерации (часть четвертая)" от 18.12.2006 N 230-ФЗ (ред. от 23.05.2018).
3. "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 N 7-ФКЗ, от 05.02.2014 N 2-ФКЗ, от 21.07.2014 N 11-ФКЗ).
4. "Окинавская хартия глобального информационного общества" (Принята на о. Окинава 22.07.2000).
5. "Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 23.04.2019).
6. Computer Misuse Act 29th June 1990 UK Public General Acts. Закон о злоупотреблении компьютерными средствами.
7. Criminal code Australia Act No. 12 of 1995 as amended. Уголовный кодекс Австралии Закон № 12 1995 года с поправками.
8. Criminal Code of Canada R.S.C., 1985, c. C-46 .Уголовный кодекс Канады.
9. French Penal Code. Уголовный Кодекс Франции.
10. Penal Code of the Federal Republic of Germany 1987. Уголовный кодекс Федеративной Республики Германия.
11. Protection of Children Act 20th July 1978 UK Public General Acts. Закон о защите детей.
12. Sexual Offences Act 2nd August 1956 UK Public General Acts. Закон о сексуальных преступлениях.
13. Terrorism Act 20th July 2000 UK Public General Acts. Закон о терроризме.
14. The Swedish Penal Code 1999. Уголовный кодекс Швеции.

15. Закон РФ от 09.07.1993 N 5351-1 (ред. от 20.07.2004) "Об авторском праве и смежных правах" Прим. Документ утратил силу с 1 января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.
16. Закон РФ от 21.07.1993 N 5485-1 (ред. от 29.07.2018) "О государственной тайне".
17. Закон РФ от 23.09.1992 N 3523-1 (ред. от 02.02.2006) "О правовой охране программ для электронных вычислительных машин и баз данных". Прим. Документ утратил силу с 1 января 2008 года в связи с принятием Федерального закона от 18.12.2006 N 231-ФЗ.
18. Федеральный закон от 02.12.1990 N 395-1 (ред. от 06.12.2011) "О банках и банковской деятельности".
19. Федеральный закон от 04.07.1996 N 85-ФЗ (ред. от 29.06.2004) "Об участии в международном информационном обмене". Прим. Документ утратил силу в связи с принятием Федерального закона от 27.07.2006 N 149-ФЗ.
20. Федеральный закон от 07.07.2003 N 126-ФЗ (ред. от 27.12.2018) "О связи".
21. Федеральный закон от 13.03.2006 N 38-ФЗ (ред. от 01.05.2019) "О рекламе" (с изм. и доп., вступающими в силу с 12.05.2019).
22. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 18.03. 2019) "Об информации, информационных технологиях и о защите информации"

Литература

1. Robert J. Sciglimpaglia. Computer Hacking: A Global Offense // Pace Yearbook of International Law/ (1991)/ №3. P.199, 231.
2. Абов А.И., Ткаченко С.Н. Международный и отечественный опят борьбы с компьютерными преступлениями. М., 2004, С.7-20.
3. Айсанов Р.М. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ //»Черные дыры» в Российском Законодательстве. Юридический журнал. – М.: «1К-Пресс», 2006, №3. С. 140.

4. Амелин Р.В. О возможном решении проблемы неполноты главы 28 УК РФ // Уголовно-исполнительная система: право, экономика, управление. - М.: Юрист, 2009, № 5. - С. 5.

5. Батурин Ю.М. Проблемы компьютерного права. – М.: Юрид. лит., 1991. С.126.

6. Борчева Н.А. Компьютерное право и ответственность за компьютерные преступления за рубежом. // На пути к информационному обществу: криминальный аспект. Сборник статей. М., 2002. С.15.

7. Ведомости Съезда Народных Депутатов Российской Федерации и Верховного Совета Российской Федерации, 1992. №42. С. 2326.

8. Вехов Б.В. Компьютерные преступления: способы совершения, методика расследования. М., 1996. С. 44; Федоров В.И. Борьба с транснациональной организованной преступностью в сфере «высоких технологий» // прокурорская и следственная практика. 1999. №3. С.31.

9. Винер Н. Кибернетика и общество // Творец и Будущее: пер. с англ. М., 2003. С.19.

10. Волеводз А.Г. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации // Российский судья. - М.: Юрист, 2002, № 9. - С. 38.

11. Волков Ю.В. Значение термина компьютерная информация // Уголовное право: стратегия развития в XXI веке. Материалы 6-й международной научно-практической конференции 29-30 января 2009г. –М.: проспект, 2009. С.415-518.

12. Гаврилов О.А. Курс правовой информатики. М., 2000; Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право /под ред. Б.Н. Топорнина. Спб., 2001.

13. Галкин А.И. Уголовная ответственность за преступления в сфере компьютерной информации // Следователь. Федеральное издание. - М., 2009, № 5 (133). - С. 4.

14. Егорышев А.С. Расследование и предупреждение неправомерного доступа к компьютерной информации: автореф. дис. канд.юрид, Самара, 2004. С.10.

15. Иванов Н.А. Глава 28 УК РФ: необходимость внесения изменений // Научные труды РАЮН. В 3-х томах. - М.: Юрист, 2008, Вып. 8 Т. 3. - С. 173-178.

16. Иванский В.П. Правовая защита информации о частной жизни граждан. Опыт современного правового регулирования. М., 1999.

17. Интернет-ресурс Судебные и нормативные акты РФ (СудАкт) https://sudact.ru/

18. Информационно-правовой портал Гарант https://www.garant.ru/

19. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: дисс. к.ю.н. Красноярск, 2002. С. 145.

20. Козлов В.Е. Теория и практика борьбы с компьютерной преступностью. – М.: Горячая линии - Телеком, 2002. С.64-74.

21. Комиссаров А. Роль криминалистики в расследовании и раскрытии компьютерных преступлений. // Конфидент. 2000. №5. С.62.

22. Комментарий к Уголовному кодексу Российской Федерации / под ред. В.И. Радченко, А.С. Михлина. Спб., 2008. С.566 (автор главы - д.ю.н., проф. А.Н. Попов).

23. Комментарий к Уголовному кодексу Российской Федерации / под ред. В.И. Радченко, А.С. Михлина. СПб., 2008. С.569.

24. Комментарий к Уголовному кодексу Российской Федерации с постатейными материалами и судебной практикой. –Ростов н/Д: Издательский центр «МарТ», 2006. – С. 675.

25. Комментарий к Уголовному кодексу РФ / под ред. д.ю.н. проф. А.Г. Королькова. М.; 2004. С.798 (авторы главы - Ю.В. Белянинова, А.М. Дедов).

26. Комментарий к УК РФ с постатейными материалами и судебной практикой / под ред. д.ю.н., проф. Улезько С.И. Ростов н/Д., 2002. С. 676 (автор главы - к.ю.н. Воронцов С.А.).

27. Костин В.п. Исследование машинных носителей информации, используемых при совершении преступлений в сфере экономики: автореф. дисс. к.ю.н. Н. Новгород, 2007. С.6.

28. Крылов В.В. Информационные компьютерные преступления. М.: Инфра-М – Норма, 1997. С.27.

29. Крылова Н.Е., Серебренникова А.В. Уголовное право современных зарубежных стран (Англии, США, Франции, Германии): Учебное пособие. М.,1997. С.184-185.; Айков Д., Сейгер К., Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. М., 1999. С.115-116.

30. Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. – М.: Новый юрист,1998.С.51.

31. Ляптунов Ю.И. Объективная сторона преступления. Уголовное право. Общая часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М ., 1997. – С. 194.

32. Ляпунов Ю.И., Пушкин А.В. Преступления в сфере компьютерной информации // Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М: Юристъ. 1998. –С. 549.

33. Мещаряков В.А. Основы методики расследования преступлений в сфере компьютерной информации: автореф. дис. канд. юр.наук. г.Воронеж, 2001, С. 14-15.

34. Мусаева У.В. Розыскная деятельность следователя по делам о преступлениях в сфере компьютерной информации: автореф. дис. канд. юрид. наук. Тула. 2002. С. 18.

35. Остроушенко А.В. Организационные аспекты методики расследования преступлений в сфере компьютерной информации: автореф. дис. Канд.юрид. наук. Волгоград, 2000, С. 4.

36. Панфилова Е.И., Попов А.С. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе». / Научн. ред. Б.В. Волженкин. Спб.: 1998.С.11.

37. Постатейный Комментарий к Уголовному кодексу РФ. / Под ред. Наумова А.В. – М., 1998.

38. Расследование неправомерного доступа к компьютерной информации: Научно-практическое пособие / Под ред. Н.Г. Шурухнова. – М., 1999. – С. 55-67.

39. Расследование неправомерного доступа к компьютерной информации: учебное пособие. Изд. 2-е, доп. и перераб. / под ред. д.ю.н., проф. Н.Г. Шурухнова. М.: Московский университет МВД России, 2004. С.95.

40. Рогозин В.Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации: автореф. Дис. Канд. Юрид. наук. Волгоград, 1998. С.4.

41. Савельев Д. Ответственность за неправомерный доступ к компьютерной информации //Российская юстиция. - 1999. -№1.

42. Справочно-правовая система КонсультантПлюс http://www.consultant.ru/

43. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: дис. канд. юрид. наук. Иркутск, 2006. С.19.

44. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы /под ред. В.А. Садовничего, В.П. Шерстюка. М., 2002. С. 23-37.

45. Уголовная ответственность за преступления в сфере компьютерной информации за рубежом. Лекция / Ястребов Д.А.; Под общ. Ред.: Каламкарян Р.А.. - 2е издание, - М.: прима-Пресс, 2004. - 62 с.

46. Уголовная ответственность за преступления в сфере компьютерной информации за рубежом. Лекция / Ястребов Д.А.; Под общ. ред.: Каламкарян Р.А.. - 2-е изд., перераб., доп. - М.: Прима-Пресс, 2004. – С. 27-28.

47. Хатунцев Н.А. Теоретические и методические основы судебной компьютерно - технической экспертизы при разрешении споров хозяйствующих субъектов: автореф. дис. к.ю.н. М., 2006. С.14.

48. Черняк Л. Это древнее слово «компьютер» // Computerworld. 2005. №10(459). С.36.