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

Институт права

Кафедра «Уголовное право и криминология»

030900.62 «Юриспруденция»
(код и наименование направления подготовки, специальности)
Уголовно-правовой
(направленность (профиль)

БАКАЛАВРСКАЯ РАБОТА

на тему «Актуальные проблемы уголовной ответственности за преступления в сфере компьютерной информации по УК РФ»

Студент Е.В. Бояров
(И.О. Фамилия) (личная подпись)

Руководитель И.Е. Третьяков
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заведующий кафедрой
«Уголовное право
и криминология» д.ю.н., доцент Т.М.Клименко
(ученая степень, звание, И.О. Фамилия) (личная подпись)

«_____»_____20_____г.

Тольятти, 2016 г.

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

Институт права

Кафедра «Уголовное право и криминология»

УТВЕРЖДАЮ
Зав. кафедрой «Уголовное право и криминология»
_____ _Т.М.Клименко_
(подпись) (И.О. Фамилия)
«____»__ _____2016 г.

ЗАДАНИЕ
на выполнение бакалаврской работы

Студент___Бояров Евгений Васильевич_____
1. Тема Актуальные проблемы уголовной ответственности за преступления в сфере компьютерной информации по УК РФ.
2. Срок сдачи студентом законченной выпускной квалификационной работы – _____
3. Исходные данные к выпускной квалификационной работе: Международно-правовые акты; Российское законодательство; Судебная практика; Статистический материал, собранный студентом при прохождении практики.
4. Содержание выпускной квалификационной работы (перечень подлежащих разработке вопросов, разделов):
Глава 1. Компьютерная информация как объект правовой защиты
Глава 2. Уголовная ответственность за преступления в сфере компьютерной информации
Глава 3. Проблемы связанные с преступлениями в сфере компьютерной информации и возможные пути их решения
5. Ориентировочный перечень графического и иллюстративного материала – правовая статистика; архивные уголовные дела.
6. Дата выдачи задания «____» _____ 201___ г.

Руководитель выпускной
квалификационной работы _____ ____И.Е.Третьяков____
(подпись) (И.О. Фамилия)

Задание принял к исполнению _____ _____Е. В. Бояров_____
(подпись) (И.О. Фамилия)

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

Институт права

Кафедра «Уголовное право и криминология»

УТВЕРЖДАЮ
Зав. кафедрой «Уголовное право и криминология»
_____ _Т.М.Клименко_
(подпись) (И.О. Фамилия)
«____» _____201_ г.

КАЛЕНДАРНЫЙ ПЛАН
выполнения бакалаврской работы

Студента_ Боярова Евгения Васильевича_____
по теме Актуальные проблемы уголовной ответственности за преступления в сфере компьютерной информации по УК РФ

Наименование раздела работы	Плановый срок выполнения раздела	Фактический срок выполнения раздела	Отметка о выполнении	Подпись руководителя
Выбор и обоснование темы ВКР	До 15 октября 2015 г.	15 октября 2015 г.	Выполнено	
Подбор библиографии	До 15 декабря 2015 г.	15 декабря 2015 г.	Выполнено	
Глава 1	С 15 января 2016 г. по 20 апреля 2016 г.	16 января 2016 г.	Выполнено	
Глава 2		13 марта 2016 г.		
Глава 3		19 апреля 2016 г.		
Введение	До 15 мая 2016 г.	25 января 2016 г.	Выполнено	
Заключение		10 мая 2016 г.	Выполнено	
Оформление ВКР	До 30 мая 2016 г.	30 мая 2016 г.	Выполнено	
Представление ВКР на кафедру	Не позднее 5 июня 2016г.	3 июня 2016 г.	Выполнено	

Руководитель выпускной квалификационной работы _____ __И.Е. Третьяков_____
(подпись) (И.О. Фамилия)

Задание принял к исполнению _____ _____Е. В. Бояров_____
(подпись) (И.О. Фамилия)

Аннотация

Объектом данной работы является компьютерная информация. Предметом исследования – преступления в сфере компьютерной информации.

Цель настоящего исследования – исследовать актуальные проблемы уголовной ответственности за преступления в сфере компьютерной информации.

Цель предопределила задачи исследования:

1. исследовать понятие «компьютерная информация»;
2. проанализировать законодательство Российской Федерации об уголовной ответственности за преступления в сфере компьютерной информации;
3. рассмотреть вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений;
4. проанализировать способы совершения преступлений в сфере компьютерной информации;
5. проанализировать проблемы и возможные пути решения в области уголовной ответственности за преступления в сфере компьютерной информации.

Структура данной работы включает введение, три главы, заключение и список использованных источников.

Содержание

Введение

Информационные технологии все глубже проникают практически во все сферы общественной жизни и благодаря этому развитию начинают играть более весомую роль в общественных отношениях. Так как информационные технологии — это сфера которая весьма быстро эволюционирует и захватывает новые сферы влияния на человеческую жизнь, то информационная безопасность приобретает невероятно важное значение. Со временем стала очевидна необходимость изучения практического использования подобных технологий, а также последствий их создания.

Отмечу, что преступления в сфере компьютерной информации обладают определенной спецификой – высокой латентностью, сложны в своевременном выявлении, подобные преступления возможно совершать на значительном расстоянии и могут возникать трудности в сборе и оформлении доказательной базы.

Возникают вопросы уголовно-правового характера преступлений в сфере компьютерной информации, например, правоприменитель иногда сталкивается со значительными затруднениями при юридической квалификации общественно опасных деяний данного вида.

В последнее время особую остроту приобрела проблема борьбы с преступлениями в сфере компьютерной информации, так как появились необходимые предпосылки, обусловленные постоянным совершенствованием компьютерных технологий и международных компьютерных сетей, которые в значительной степени способствуют облегчению в совершении подобных преступных деяний как внутри государства, так и на международном уровне. Совершение информационных преступлений возможно на значительном расстоянии от объекта преступления буквально за несколько секунд.

Законодательство Российской Федерации, в частности Уголовный кодекс Российской Федерации [1] (далее – УК РФ), предусматривает уголовную ответственность за преступления в сфере компьютерной информации (Глава 28), хотя содержит всего три статьи (ст. 272 – 274 УК РФ).

Учитывая вышеизложенное, становится очевидна актуальность рассмотрения уголовно-правовой характеристики преступлений в сфере компьютерной информации, в частности выявления актуальных проблем уголовной ответственности в указанной области.

Объектом исследования является компьютерная информация. Предметом исследования – преступления в сфере компьютерной информации.

Цель настоящего исследования – исследовать актуальные проблемы уголовной ответственности за преступления в сфере компьютерной информации.

Цель предопределила задачи исследования:

1. исследовать понятие «компьютерная информация»;
2. проанализировать законодательство Российской Федерации об уголовной ответственности за преступления в сфере компьютерной информации;
3. рассмотреть вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений;
4. проанализировать способы совершения преступлений в сфере компьютерной информации;
5. проанализировать проблемы и возможные пути решения в области уголовной ответственности за преступления в сфере компьютерной информации.

[1] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.03.2016) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

Структура исследования включает введение, три главы, заключение и список использованных источников.

Глава 1. Компьютерная информация как объект правовой защиты

1.1 К вопросу о понятии компьютерной информации

Проводя анализ категории «компьютерная информация» следует подметить, что преступления, которые подпадают под данное понятие, являются одним из срезов информационной преступности, однако нередки случаи, когда зарубежные и отечественные издания относят их к компьютерным или киберпреступлениям. Однако на мой взгляд это не совсем корректно, ибо данные преступления зачастую не содержат все необходимые криминальные проявления, связанные с использованием компьютерных сетей.

Кесареева Т. П. утверждает, что неотъемлемой частью компьютерной преступности являются преступления, совершенные непосредственно с использованием компьютерных сетей, а также подобные преступления обладают некой собственной спецификой[2]. Однако, следует отметить, что перечисленные выше преступления не обладают юридической природой. Тщательно изучив учебную и научную литературу, можно прийти к определенному выводу - большинство авторов склонны считать, что компьютерные преступления образуют деяния, непосредственно относящиеся к несанкционированному доступу к серверам, сетям и машинным ресурсам, а также в большинстве своем направлены на уничтожение или повреждение информации, либо должны нарушить привычное состояние компьютерных сетей или компьютеров[3].

Я рассматриваю систему преступлений совершаемых с использованием компьютерных сетей в более широком смысле и считаю, что в том числе

---

[2] Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: Автореф. дис. ... канд. юрид. наук. М., 2002. С. 6.

[3] Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореф. дис. ... канд. юрид. наук. Елец, 2006. С. 13.

должны быть включены преступные деяния, связанные также с санкционированным доступом к серверам и компьютерным сетям[4].

Система преступлений, совершаемых с использованием компьютерных систем не должна отождествляться с киберпреступностью, которая по структуре своей является уже компьютерной преступности.

Киберпреступоностью является совокупность преступлений, которые совершаются в киберпространстве с использованием компьютерных сетей или компьютерных систем, а также других средств, предоставляющих доступ к киберпространству, в рамках компьютерных сетей или систем и направленные против компьютерных систем, данных или сетей[5].

В настоящее время термин «информационная преступность» довольно часто используют различные авторы для определения преступных проявлений в информационной сфере, где информационная связь выступает к преступности как существенный признак.

В теории криминологии на данный момент нет единого мнения по вопросу структуры информационной преступности, в связи с этим в юридической литературе все больше превалирует мнение о том, что понятие информационные преступления требует более лучшего, расширенного толкования.

Одно и тоже преступление при наличии ряда определенных условий можно отнести как к информационным, так и нет. К примеру, нарушение авторских и смежных прав, мошенничество, вымогательство – данные преступления направлены на различные объекты уголовно-правовой охраны, но проведя анализ способа их совершения в каждом конкретном случае их можно, с определенной долей условности, отнести к информационным.

В диссертационной работе Третьякова А. Н. предлагается определять структуру информационных преступлений основываясь на характере

---

[4] Доржиев А.В. Уголовно-правовые меры противодействия преступлениям, совершаемым в предпринимательской сфере: Дис. ... канд. юрид. наук. М., 2010. С. 154 - 155.

[5] Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. ... канд. юрид. наук. Владивосток, 2005. С. 36.

содержащихся в них угроз. Данный автор представляет три группы подобных преступлений, в ядре классификации которых лежит угроза:

- возможность воздействия некачественной информации на личность, общество и государство;

- воздействие на информацию посторонних лиц произошедшее не санкционировано и неправомерно, а также подобного рода воздействие на производство информации и информационные ресурсы;

- угроза информационным правам и свободам личности. К примеру вмешательство в производство, распространение, поиск, получение, передачу или использование информации;

Однако, некоторые ученые заявляют, что присутствует связь информации и преступности, которую можно проследить через объект и предмет противоправного посягательства.

Суслопаров А.В. пишет: «Предметом является информация, которая не имеет какой-либо определенной материальной формы и не зависит от своего материального носителя. В каждом отдельном случае преступного посягательства информация хранится на таком носителе, однако не имеет строгой связи с ним»[6].

Мое мнение о предмете подобных преступлений является традиционным: предмет определен в теории уголовного права в виде неких объектов материального мира. Информацию, на мой взгляд, нужно определять как предмет уголовно-правовой охраны, а не предмет состава преступления. Именно таким образом информацию исследуют в абсолютном большинстве работ по уголовному праву.

Итак, основную категорию информационных преступлений составляют в основном преступления, описанные нормами Гл. 28 УК РФ[7] («Преступления в сфере компьютерной информации»), в которых

---

[6] Суслопаров А.В. Информационные преступления: Автореф. дис. ... канд. юрид. наук. Красноярск, 2008. С. 8, 13 - 14.

[7] Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.03.2016) // Собрание законодательства РФ. 1996. № 25. Ст. 2954.

непосредственным объектом преступлений выступают общественные отношения, возникающие в сфере компьютерной информации или обеспечивающие безопасность компьютерной информации. Однако, данную главу не стоит считать исчерпывающей, так как мы можем причислить еще большой список преступных деяний, которые предусмотрены разными статьями глав УК РФ. Исключениями не являются даже преступления против жизни и здоровья, так как судебная практика знает не мало случаев, когда с помощью распространения информации совершались убийства или, причинялся вред здоровью. Стоит отметить, что в последние годы все чаще начинают использовать компьютерные сети. К примеру, сейчас в сети интернет имеется огромное количество рекомендаций и инструкций направленные на подавление воли человека.

Не редки случаи, когда при использовании вредоносной программы в компьютерных сетях похищают различные реквизиты банковских карт и платежных систем с последующим хищением денег с электронных счетов.

Итак, для уголовно-правовой характеристики преступлений в сфере компьютерной информации очень важное значение имеет само понятие «компьютерная информация», и российский законодатель закрепил данное понятие в Примечании 1 ст. 272 УК РФ: «Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи».

1.2 Законодательство РФ об уголовной ответственности за преступления в сфере компьютерной информации

В 1979 году в городе Вильнюсе было зарегистрировано первое преступление с использованием компьютера совершенное на территории СССР. Данное преступление было занесено в международный реестр

подобного рода правонарушений и является отправной точкой развития нового вида преступности в стране[8].

Государство практически сразу начало искать возможность уголовно-правового регулирования подобного рода преступлений.

Можно выделить следующие этапы развития:

- проект закона РСФСР «Об ответственности за правонарушения при работе с информацией» разработанный и представленный 06.12.1991 года, в нем предлагали ввести в УК РСФСР нормы об ответственности за совершение преступлений, связанных с компьютерной информацией[9];

- Постановление Верховного Совета Российской Федерации от 23.09.1992 года № 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных»[10], пунктом 5 которого предписывалось Правительству РФ до 31.12.1992 года внести в установленном законом порядке на рассмотрение Верховного Совета Российской Федерации проекты законов Российской Федерации о внесении изменений и дополнений в Гражданский кодекс РСФСР, в Уголовный кодекс РСФСР, другие законодательные акты, связанные с вопросами правовой охраны программ для электронных вычислительных машин и баз данных;

- в 1994 году завершилась разработка проекта закона о внесении дополнений в УК РСФСР, в котором устанавливалась ответственность за: незаконное овладение программами для ЭВМ, файлами и базами данных; фальсификацию или уничтожение информации в автоматизированной системе; незаконное проникновение в автоматизированную информационную систему (АИС), совершенное путем незаконного завладения парольно-ключевой информацией, нарушения порядка доступа или обхода механизмов программной защиты информации с целью ее

---

[8] Батурин Ю.М. Проблемы компьютерного права. М.: Юрид. лит., 1991. С. 126.

[9] Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М.: Новый юрист, 1998. С. 51.

[10] См.: Ведомости Съезда Народных Депутатов Российской Федерации и Верховного Совета Российской Федерации. 1992. № 42. Ст. 2326. Утратил силу.

несанкционированного копирования, изменения или уничтожения; внесение и распространение «компьютерного вируса»; нарушение правил, обеспечивающих безопасность АИС[11];

- в январе – феврале 1995 года разработали и опубликовали проект УК РФ, в котором была предусмотрена Глава 29 «Компьютерные преступления»;

- принятие и введение в действие с 01.01.1997 года Уголовного кодекса Российской Федерации, в котором имеется Глава 28 «Преступления в сфере компьютерной информации».

[11] Курушин В.Д., Минаев В.А. Компьютерные преступления и информационная безопасность. М.: Новый юрист, 1998. С. 52.

Глава 2. Уголовная ответственность за преступления в сфере компьютерной информации

2.1 Неправомерный доступ к компьютерной информации

Статья 272 УК РФ регламентирует уголовную ответственность за неправомерный доступ к охраняемой законом компьютерной информации, а именно – содержащейся на машинном носителе информации, в электронно-вычислительной машине (ЭВМ) или их сети, при этом должно произойти уничтожение, блокировка, копирование или модификации информации, либо дезорганизация работы ЭВМ или их сети[12]. Информационная безопасность является объектом подобного рода преступления, в свою очередь предметом является компьютерная информация, охраняемая законом.

Компьютерная информация представляет из себя сведения, которые содержатся на каком-либо машинном носителе информации. К таким можно относить: жесткий диск типа Винчестер, дискеты – информационные накопители в виде гибких магнитных дисков, кассетные магнитные ленты, оптические диски, а также флеш-картах памяти. Стоит отметить, что носителями информации подобного рода возможно манипулировать только с помощью ЭВМ.

Согласно статье 272 УК РФ уголовно-правовая охрана обеспечивается только охраняемой законом информации. Но так как диспозиция статьи является бланкетной, то чтобы определить какого рода информация имеется ввиду, необходимо обратиться к другому законодательству. Исходя из терминологии ФЗ «Об информации, информатизации и защите информации» вся охраняемая информация разграничивается на относящуюся к государственной тайне, и конфиденциальную. Объективной стороной подобного рода преступлений является неправомерный доступ к компьютерной информации. Неправомерный доступ подразумевает под собой способы получения или просмотра информации, совершающиеся с

[12] Борзенкова, Г.Н. Курс уголовного права в пяти томах. Том 4. Особенная часть / Под ред. Г.Н. Борзенкова, В.С. Комисарова. М., - 2002. - С. 580

игнорированием регламентированного порядка обращения к защищаемой информации, либо без согласия владельца или собственника информации.

Классификация незаконных способов ознакомления с компьютерной информацией в основном происходит по двум болим группам:

- традиционные способы – противозаконный доступ осуществляется без использования каких-либо компьютерных программ;

- неправомерное проникновение к компьютерной информации путем использования достижений науки и техники.

К первой группе следует относить похищение непосредственно носителей информации, а также различных средств, предназначенных для хранящих информации. Ко второй группе следует относить перехват информации: электромагнитный (задействует электромагнитное излучения при работе компьютерных систем не требующая контакта с ними); в кабельных линиях; перехват аудио и видео сигналов.

С использованием программ осуществляется большинство способов незаконного доступа к компьютерной информации.

Большинство способов незаконного доступа к компьютерной информации происходит с использованием программ. К незаконному доступу с использованием компьютера можно отнести:

- задействуют чужие пароли, коды, так называемую электронную «маскировку»;

- производят электронную «уборку мусора» - исследую файлы на компьютере, которые были удалены пользователем, однако все еще полностью не стерлись из компьютерной памяти;

- противоправный перехват компьютерной информации, а также подключение к зашифрованным каналам компьютерной связи[13];

Предусмотренный ч. 1 ст. 272 УК РФ состав преступления является материальным, соответственно необходимо наступление определенных

[13] Айков Д.Н. Компьютерные преступления: Руководство по борьбе с компьютерными преступлениями (Пер. с англ.) / Д. Айков, К. Сейгер, У. Фонсторх. - М., 2009. - С. 107.

последствий для признания преступления оконченным. Такими последствиями являются: уничтожение, блокирование, модификация либо копирование информации. Уничтожением информации в данном случае будет являться потеря информации, которая не поддается восстановлению, становится невозможным ее использование и прочтение. При блокировании информация хоть и сохраняется физически, однако становится невозможным получить к ней доступ и использовать. Модификацией информации следует признать полное или же частичное изменение первоначальной информации. Копирование информации выражается в создании хотя бы одной копии, вне зависимости от характера ее физического носителя - бумажного, магнитного, лазерного или иного при наличии сохраненного оригинала информации.

Субъективная сторона подобных преступлений выражена прямым умыслом. Правонарушитель явно понимает, что получает неправомерный доступ к информации, при этом предвидит возможность, либо неизбежность наступления последствий, указанных непосредственно в диспозиции статьи[14].

Субъект - общий, вменяемое лицо, достигшее 16-летнего возраста.

Часть 3 статьи 272 в свою очередь предусматривает квалифицирующие признаки:

деяние, совершенное группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

В данном случае имеется специальный субъект, который использует служебное положение, таким субъектом может являться должностное лицо, либо государственный и муниципальный служащий, который не является должностным лицом, а также любое другое лицо использующее свое положение в организации, работником которой оно является.

---

[14] Иногамовой-Хегай, Л.В. Уголовное право. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, А.И. Рарога, А.И. Чучаева. - М., 2008. - С. 308.

2.2 Создание, использование и распространение вредоносных компьютерных программ

Такие преступления относят к наиболее общественно опасным деяниям из числа преступлений, которые посягают на компьютерную информацию и это выражено в размере и конструировании санкций, описанных в части 1 статьи 273 УК РФ.

Именно различные вредоносные программы наносят самый большой вред собственникам, владельцам и пользователям информационных ресурсов и компьютерных средств[15].

Статья 273 УК РФ предусматривает уголовную ответственность за создание и распространение компьютерных вирусов, но в действительности предмет данной статьи представляется шире и также включает в себя иные вредоносные программы.

На данный момент времени существует несколько десятков тысяч программ-вирусов и их количество безостановочно растет с каждым днем.

Только путем совершения активных действий возможно выполнение объективной стороны данного преступления. Хочется отметить что создание, использование и распространение вредоносных компьютерных программ будет считаться выполненным только с момента непосредственного создания такой программы, внесение каких-либо изменений в уже существующие программы, а также использования или распространения программы. Однако объективная сторона состава преступления не предусматривает наступления определенных последствий, но нужно учитывать, что подобного рода программы должны нести в себе угрозу уничтожения, блокировки, модификации и копирование информации, а также нарушать работу компьютерных программ. Противоправное деяние будет признано оконченным при совершении даже одного действия предусмотренного диспозицией статьи, при этом программа не обязательно должна причинить

[15] Борзенков Г.Н. Курс уголовного права в пяти томах. Том 4. Особенная часть / Под ред. Г.Н. Борзенкова, В.С. Комисарова. М., 2002. - С. 200.

реальный вред информационным ресурсам[16]. В специализированной литературе можно встретить противоположные мнения относительно характера субъективной стороны рассматриваемого преступления. Одни авторы считают, что подобные преступления возможно совершить только с прямым умыслом, иные - исключительно по неосторожности, третьи - только с косвенным умыслом[17].

Если был установлен прямой умысел в совершенном преступлении, то его следует квалифицировать по иным статьям УК РФ в соответствии с поставленной целью и наступившими последствиями.

Не стоит загонять субъективную сторону преступления в рамки только прямого умысла, так как возможны случаи, когда лицо не желало, однако сознательно допускает наступление вредных последствий или относится к ним безразлично. Дело в том, что в силу специфики работы электронно-вычислительной техники дальнейшее распространение такой программы вероятно, но не неизбежно. Поэтому субъективная сторона преступления может характеризоваться как прямым, так и косвенным умыслом.

Субъект преступления - лицо, достигшее возраста 16 лет.

2.3 Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Данное правонарушение выражается в невыполнении предписанных правил эксплуатации электронной вычислительной техники. Данные правила находят свое отражение в ведомственных нормативных актах, установленных государством, а также отдельными юридическими лицами, которые являются собственниками или законными владельцами

[16] Малько А.В. Большой юридический словарь / под ред. А. В. Малько - М.: Проспект. - 2009. с. 308.
[17] Ляпунова Ю.И. Уголовное право. Особенная часть/под ред. Н.И.Ветрова и Ю.И.Ляпунова. М., - 2008. - С. 558.

информационно-телекоммуникационных сетей. Данная норма является бланкетной и в связи с этим для правильности определения объективной стороны нужно установить конкретный нормативный или же иной акт, предписания которого были нарушены виновным лицом[18].

Объективная сторона преступления раскрывается как в активном действии, так и бездействии, сопряженном с нарушением строго установленных правил. Стоит подчеркнуть, что непосредственное содержание этих правил описано в нормативных актах иных отраслей права, таких как – законы, правила, инструкции.

Подобные правила могут быть представлены в общих требованиях по технике безопасности и эксплуатации компьютерного оборудования, а также в специальных правилах, которые регламентируют особые рабочие условия, такие как – продолжительность времени, последовательность произведения операций, максимальные нагрузки.

По составу данное преступление сформулировано как материальное. Преступление будет признано оконченным с момента наступления одного из последствий, перечисленных в статье 274 УК РФ, а именно – уничтожение, блокировка, модификация и копирование информации, причинившее крупный ущерб.

Субъективная сторона данного состава может быть выражена виной в форме умысла и неосторожности.

Субъектом преступления является специальное, физически вменяемое лицо, достигшее 16 лет и имеющее доступ к компьютерной системе.

В юридической литературе достаточно популярна мысль о том, что компьютерное мошенничество необходимо квалифицировать исключительно по статье 159 УК РФ (Мошенничество) либо, исходя из обстоятельств дела по статье 158 УК РФ. Следует отметить, что приоритет отдается преступлениям против собственности, в которых компьютер или

[18] Борзенков Г.Н. Курс уголовного права в пяти томах. Том 4. Особенная часть / Под ред. Г.Н. Борзенкова, В.С. Комисарова. М., -2002. - С. 490.

компьютерные сети использовались в качестве орудия или средства совершения.

На данный момент времени дискуссионным остается вопрос квалификации преступления со сложным составом, а именно вопрос о том, охватываются ли ими вышеперечисленные простые составы или необходима квалификацию по совокупности преступлений.

Глава 3. Проблемы связанные с преступлениями в сфере компьютерной информации и возможные пути их решения

3.1 О возможном решении проблемы неполноты главы 28 УК РФ

Глава 28 УК РФ появилась в 1996 году и ее появление на фоне стремительного развития информационных технологий было своевременным и весьма обоснованным. Однако, глава 28 УК РФ регулирует достаточно новые общественные отношения, из-за чего в понятийно сфере имеются многочисленные недостатки. Отечественные юристы многократно затрагивали в своих научных трудах проблемы в понятийном аппарате главы 28 УК РФ, но конкретно в этой работе я бы хотел затронуть более углубленную проблему, такую как – неполнота объективной части статей 272, 273, 274 УК РФ.

В основу классификации преступлений, указанных в главе 28 УК РФ, лег общий для УК РФ подход, т.е. на основании объективной стороны. Соответственно рассматриваются угрозы компьютерной информации не с точки зрения ее свойств, которые нарушаются по результату неправомерных действий (бездействия), а с точки зрения непосредственно самих этих действий.

Стоит отметить, что законодательно закрепить полный перечень действий, которые угрожают правоотношениям в сфере компьютерной информации весьма проблематично, особенно в современных условиях непрекращающегося развития информационных технологий, а также средств и способов обработки информационных данных и доступа к ним. Также, на мой взгляд, практически невозможно закрепить полный перечень общественно опасных последствий, наступление которых возможно в результате совершения неправомерных действий.

К примеру, чтение информации с экрана монитора формально не подпадает ни под одно из перечисленных понятий (уничтожение,

блокирование, копирование, модификация), но может нарушать права владельца информации в случае, когда данная информация является коммерческой или личной тайной[19].

Были выработаны три центральных свойства информации, такие как: доступность, целостность и конфиденциальность. Их разительное отличие от иных свойств в том, что они не присущи информации как таковой, а проявляются только в результате принятия мер иного организационного характера.

Обретя перечисленные свойства определенная информация может и лишиться их в результате какого-либо внешнего воздействия. Подобное воздействие может быть, как результатом события (например, в результате стихийного бедствия был уничтожен банк данных - потеря целостности и доступности), так и действия.

Информация обладающая какими-либо из перечисленных свойств обладает наибольшей ценностью и соответственно неправомерные действия нарушающие такие свойства наносят собственнику подобной информации значительный ущерб, а значит и общественным отношениям в соответствующей области[20].

Глава 28 УК РФ по своей сути предназначена обеспечивать непосредственно уголовно-правовую защиту вышеперечисленных свойств. Хочется отметить, что другие, второстепенные свойства информации в защите такого рода не нуждаются, так как идеальность и неисчерпаемость, к примеру, являются неотъемлемыми по своей природе, а достоверность и объективность либо присутствует, либо нет, но при их изменении – это будет уже совершенно другая информация.

---

[19] См., напр.: Расследование неправомерного доступа к компьютерной информации: Учебное пособие. Изд-е 2-е, доп. и перераб. / Под ред. д.ю.н., проф. Н.Г. Шурухнова. М.: Московский университет МВД России, 2004. С. 95.

[20] См.: Шнайер Б. Секреты и ложь. Безопасность данных в цифровом мире. СПб.: Питер, 2003; Соколов А.В., Степанюк О.М. Защита от компьютерного терроризма. СПб.: БХВ-Петербург, 2002; Щеглов А.Ю. Защита компьютерной информации от несанкционированного доступа. СПб.: НиТ, 2004.

Внимательно анализируя статьи 28 главы УК РФ можно заметить, что статьями охраняются главным образом три свойства, а именно: при копировании компьютерной информации происходит нарушение конфиденциальности, при модификации происходит нарушение целостности, а при блокировке и уничтожении происходит соответственно нарушение доступности.

Однако, нарушить эти свойства можно и другими способами, к примеру, конфиденциальность можно нарушить просмотром информации с дисплея или других средств визуального отображения, с помощью перехвата электромагнитных излучений, либо виброакустических сигналов; доступность в свою очередь можно нарушить хищением технический средств с хранящийся в них информацией, либо иных носителей информации[21].

Кроме всего прочего кроме несанкционированного доступа к компьютерной информации и использования вредоносных программ появляются все более новые способы для копирования, уничтожения, блокировки и модификации информации. К таким новым способом можно отнести социальный инжиниринг – правонарушитель, совершая обманные действия провоцирует владельца компьютера выложить в открытый доступ конфиденциальную информацию. В данном случае действия владельца компьютера можно квалифицировать по статье 274 УК РФ, но в свою очередь провести квалификацию действий преступника по статье 272 УК РФ в практических условиях представляется весьма затруднительным.

На мой взгляд, целесообразнее было бы использовать подход, при котором уголовная ответственность устанавливается за нарушение конфиденциальности, доступности и целостности информации могла бы быть единой независимо от способов совершения преступлений. В качестве квалифицирующего признака могли бы выступать, из-за их общественной

[21] См., напр., о возможных каналах утечки информации руководящий документ Государственной технической комиссии при Президенте РФ «Защита от несанкционированного доступа к информации» // Справочно-правовая система «КонсультантПлюс».

опасности, отдельные способы, такие как, создание и распространение вредоносных программ.

3.2 Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества

Для своевременной и эффективной борьбы с киберпреступностью необходим соответствующий правовой механизм и правовое обеспечение, так как установление состава преступления возможно лишь при предусмотренной уголовной ответственности за подобные правонарушения. Важным для определения состава преступления также является умышленность его совершения, либо неосторожность. Следовательно, преступной можно считать деятельность, если в установленном законом порядке ее осуществление не является санкционированным государством.

Согласно статье 272 УК РФ уголовное наказание следует за неправомерный доступ к охраняемой законом компьютерной информации, при условии, что это действие повлекло за собой уничтожение, блокирование, модификацию или копирование компьютерной информации. Соответственно предметом подобных преступлений будет являться охраняемая законом компьютерная информация. Данная информация должна быть на компьютере, мобильном средстве связи, т.е. носителе информации или ее программном обеспечении.

Статья 273 УК РФ находящаяся в главе 28 УК РФ предусматривает уголовную ответственность за создание, распространение или использование компьютерных программ либо другой компьютерной информации, если данные действия направлены на несанкционированное уничтожение, блокирование, модификацию, копирование компьютерной информации, а также нейтрализацию средств защиты компьютерной информации.

Подобного рода преступления с объективной стороны выражаются в совершении какого-либо из данных действий:

- создаются компьютерные программы или другая компьютерная информация, которая априори предназначается для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации;

- использование таких компьютерных программ или такой компьютерной информации;

- данные компьютерные программы или информация распространяются.

В статье 274 УК РФ предусмотрена уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, однако стоит принять во внимание, что неправомерный доступ к компьютерной информации, создание и распространение вредоносных программ будет являться подготовительной стадией или покушением при совершении иных преступлений, корыстных в первую очередь.

Следует отметить, что кроме статей 272 – 274 УК РФ ответственность за совершение преступлений, которые связаны с использование информационных технологий предусмотрены в статьях 159.6 УК РФ «Мошенничество в сфере компьютерной информации» и статье 159.3 УК РФ «Мошенничество с использованием платежных карт», а также других[22].

В судебной и следственной практике могут возникнуть вопросы, связанные с отграничением неправомерного доступа к компьютерной информации от такого преступления, как, например, нарушение неприкосновенности частной жизни (ст. 137 УК РФ).

Приведем пример судебной практики по ч. 1 ст. 137 УК РФ. Приговор мирового судьи судебного участка № 13 Кировского района г. Перми от 07.12.2015 по делу № 1-103/2015[23].

---

[22] Статьи 159.3 и 159.6 УК РФ введены Федеральным законом от 29.11.2012 N 207-ФЗ.

[23] Приговор мирового судьи судебного участка № 13 Кировского района г.Перми от 07.12.2015 по делу № 1-103/2015// Росправосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-13-kirovskogo-rajona-g-permi-s/act-225265116/ (дата обращения: 10.04.2016).

Суд, рассмотрев материалы уголовного дела, установил следующее. Обвиняемый «ФИО» в вечернее время, действуя умышленно и незаконно, в связи с возникшей у него к потерпевшей «ФИО» личной неприязнью, вызванной ревностью, с целью распространения сведений о частной жизни лица, составляющих личную тайну для публичной демонстрации, используя свой мобильный телефон «LG», подключенный к сети Интернет, достоверно зная, что данная сеть является средством массовой информации, используемым неопределенным кругом лиц, через свою страницу в социальной сети «В контакте», действуя в нарушение ч. 1 ст. 23, ч. 1 ст. 24 Конституции Российской Федерации, ст. 12 Всеобщей декларации прав человека и ст. 17 Международного пакта о гражданских и политических правах, гарантирующих права на неприкосновенность частной жизни, личной тайны, желая создать о «ФИО» перед неопределенным кругом лиц мнение, как о женщине вульгарного поведения, умышленно разместил в группе (сообществе) «Курицы & Бабники", фотографии с изображением потерпевшей «ФИО» без ее согласия, в том числе содержащие интимные изображения ее тела, составляющие личную тайну «ФИО», то есть незаконно распространил сведения о её частной жизни, публично демонстрируя указанную информацию в средствах массовой информации в сети Интернет.

В связи с преступными действиями «ФИО» о наличии и содержании указанных фотографий, которые составляют сведения о частной жизни, потерпевшей «ФИО», являются ее личной тайной, стало известно неопределенному кругу лиц, чем потерпевшей «ФИО» причинен моральный вред. По просьбе потерпевшей «ФИО» фотографии с ее изображением в группе (сообществе) «Курицы & Бабники» были удалены службой технической поддержки социальной сети «В контакте».

Рассмотрев материалы уголовного дела, суд признал виновным «ФИО» в совершении преступления, предусмотренного по ч. 1 ст. 137 УК РФ.

Объектом этого преступления выступает неприкосновенность личного суверенитета человека, сфера его частной жизни и личных отношений.

Между тем трудно не признать, что неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, составляющие его личную или семейную тайну, представляет собой не что иное, как специфическую разновидность сбора этих сведений, иными словами, совершение действий, образующих оконченный состав нарушения неприкосновенности частной жизни. Поэтому неправомерный доступ к компьютерной информации, содержащей сведения о частной жизни лица, совершенный с прямым умыслом и из корыстной или иной личной заинтересованности, при условии причинения вреда правам и законным интересам граждан, квалифицируется по совокупности со ст. 137 УК РФ.

В этой части я предлагаю подробнее рассмотреть вопрос правового регулирования составов преступления, которые можно отнести к мошенничеству с применением каких-либо компьютерных технологий совершаемые с обманным намерением получить финансовую выгоду для самого себя либо третьих лиц.

Понятие мошенничества в кибернетической среде имеет специфический смысл. Согласно Конвенции о киберпреступности (ETS N 185)[24], принятой Советом Европы 23 ноября 2001 года в г. Будапеште, это лишение другого лица собственности путем какого-либо ввода, изменения, стирания или подавления компьютерных данных, а также иное вмешательств в нормальное рабочее состояние компьютерной системы заведомо направленное на неправомерное извлечение для себя либо третьих лиц экономической выгоды.

Можно смело утверждать, что подобные преступления развиваются и имеют хорошую тенденцию распространения. Не лишним будет заметить, что подлог сопряженный с использованием компьютерных технологий также включает в себя действия являющиеся противоправными, такие как ввод, изменение, удаление или блокировка данных, которое влечет впоследствии

[24] Конвенция о преступности в сфере компьютерной информации (ETS № 185): заключена в г.Будапеште 23.11.2001 // доступ из справ.-правовой системы «КонсультантПлюс».

нарушение аутентичности данных, с тем намерением, чтобы эти данные были рассмотрены или использованы в качестве аутентичных при наличии каких-либо юридических целей, в независимости от того, может ли пользователь непосредственно прочитать или понять эти данные.

Законодатель выделил мошенничество в сфере компьютерной информации (статья 159.6 УК РФ) и основывался он на том, что необходима уголовная ответственность в тех случаях, когда при хищении или приобретении прав на чужое имущество это связано с вмешательством в компьютерные системы.

Отмечу, что подобного рода правонарушения могут совершаться путем обмана конкретного человека, либо злоупотреблением доверия, а также тайно, путем получения доступа к компьютерной системе и совершения действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество.

При внимательном рассмотрении редакции статьи 159.6 УК РФ «Мошенничество в сфере компьютерной информации» можно понимать – «хищение чужого имущества или приобретение права на чужое имущество путем ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей...».

При этом квалифицирующими признаками являются: осуществление преступления группой лиц по предварительному сговору, а равно с причинением значительного ущерба гражданину; совершение преступления лицом с использованием своего служебного положения, а равно в крупном размере; совершение преступления организованной группой либо в особо крупном размере. Крупным размером в данном случае будет являться стоимость имущества, более одного миллиона пятьсот тысяч рублей, а особо крупным - шесть миллионов рублей.

Президиумом Верховного Суда Российской Федерации в Обзоре судебной практики по применению Федерального закона от 29 ноября 2012 г. N 207-ФЗ дано разъяснение по уголовно-правовым составам статей 159.1 - 159.6 УК РФ. Так, в Обзоре определено, что данные составы необходимо понимать, как специальные разновидности общего состава мошенничества, закрепленного в статье 159 УК РФ «Мошенничество».

В этой связи можно сделать вывод, что юридическая модель ст. 159 УК РФ является основой (родовой частью), а производные от нее «новые» составы - видовыми уголовно-правовыми конструкциями (составляющими). При этом родовая и видовые части в совокупности направлены на создание широкого юридического поля для противодействия мошенничеству, совершаемому в различных сферах деятельности и различными способами. Таким образом, ст. 159.6 УК РФ по составу преступления является «специальным» видом мошенничества и в то же время одним из видов или/и самостоятельных форм хищения.

Следует отметить, что объективной стороной мошенничества (статья 159 УК РФ) предполагает выясненный способ обмана и злоупотребление доверием. Однако в диспозиции статьи 159.6 УК РФ не указано какие именно существуют способы обмана и злоупотребления. При квалификации преступления как мошенничество законодатель предусмотрел конкретные способы его совершения, а именно: удаление, блокирование, модификацию компьютерной информации. Подобный способ совершения преступного деяния предполагает отсутствие личного контакта лица и потерпевшей стороны.

Субъект преступления совершает его путем использования технических и программных средств. Итак, объективная сторона составов преступлений статей 159 и 159.6 УК РФ по вышеописанным логико-конструктивным признакам не совпадает, так как стоит напомнить, что в диспозиции статьи 159 УК РФ указано следующее – «Мошенничество, то

есть хищение чужого имущества или приобретение права на чужое имущество путем обмана или злоупотребления доверием».

Следует сказать, что именно те обстоятельства, что мошенничество в сфере компьютерной информации не совпадают по объективной стороне состава с привычным мошенничеством (статья 159 УК РФ), что его совершение производится не путем обмана или злоупотреблением доверия конкретного человека, при этом дистанционно – стали основой выделения на законодательном уровне данного состава в отдельную статью УК РФ. Состав статьи 159.6 УК РФ в большинстве своем не представляет частного случая мошенничества, в это же время редакция статьи позволит нам прийти к выводу о выделении самостоятельного способа или формы хищения.

Основываясь на анализе состава преступления, которым будет являться мошенничество в особо крупном размере (ч. 4 статья 159.6 УК РФ), можно сказать что оно в большинстве своем копирует основной состав статьи 159 УК РФ, при этом дополняются несколькими факультативными признаками объективной стороны, такими как: совершаемое с использованием платежных карт, в сфере компьютерной информации и другое.

В конечном итоге при конструировании этого «специального» мошенничества на практике возникают некоторые сложности с квалификацией. Таким образом можно сказать, если есть указание на один из факультативных признаков состава «специального» мошенничества, такие как средство, способ или орудие, то это не исключает его квалификацию по иному составу мошенничества. Таким образом мошенничество в сфере кредитования может быть совершено с платежными картами.

Также следует отметить, что дополнительным объектом таких преступлений является компьютерная информация, с использованием которой виновный производит осуществление обманных действий, в следствии чего происходит завладение имуществом или приобретает право на соответствующее имущество. Из вышеизложенного следует, что незаконный доступ к охраняемой законом компьютерной информации и

иные противоправные действия в соответствующей сфере нуждаются в квалификации по совокупности со статьями 272, 273 УК РФ.

В связи с этим нередко возникает дилемма в отношении правильности установления преступления в действиях виновного лица.

Если совершается хищение с использованием платежных карт и при этом потерпевший лишается финансов из-за незаконного получения доступа к персональной информации и информации о платежной системе, и, следовательно, охраняемой законным интересам компьютерной информации, посредством вмешательства в работу средств хранения, обработки или передачи компьютерной информации, квалификация должна быть произведена по статьям 159.3 УК РФ «Мошенничество с использованием платежных карт» и 159.6 УК РФ «Мошенничество в сфере компьютерной информации» по совокупности со статьями 272 или 273 УК РФ. Хотелось бы обратить внимание на то, что вышеописанный способ хищений является не каким-либо абстрактным, а наиболее популярным способом хищения.

Таким образом, вид мошенничества, предусмотренный статьей 159.6 УК РФ, является частным случаем основного состава мошенничества. Введение отдельного состава мошенничества в сфере компьютерной информации позволило отчасти конкретизировать и дополнить уголовное законодательство, произвести дифференциацию специальных (частных) составов мошенничества, однако проблему упрощения и однозначности квалификации не решило.

В этой связи следует согласиться с выводом В.И. Гладких о том, что редакция введенной Федеральным законом от 29 ноября 2012 года № 207-ФЗ статьи 159.6 УК РФ «Мошенничество в сфере компьютерной информации» выглядит весьма странной и нелогичной[25].

В результате, считаем, цель выделения в УК РФ специальных составов преступлений (ст. ст. 159.3, 159.6) на практике не достигнута, хотя уже

[25] Гладких В.И. Компьютерное мошенничество: а были ли основания его криминализации? // СПС "КонсультантПлюс".

прошло более двух лет со дня их введения в УК РФ. Однако на практике данная норма применяется далеко не всегда. Кроме того, следует сказать, что в случае несанкционированного снятия финансовых средств с использованием компьютерных технологий с точки зрения уголовного права такое деяние можно квалифицировать как кражу, так как преступление совершается не путем обмана или злоупотребления доверием.

Итак, выделение мошенничества в сфере компьютерной информации в самостоятельный состав преступления (ст. 159.6 УК РФ) основывается на необходимости установления уголовной ответственности в тех случаях, когда хищение или приобретение права на чужое имущество непосредственно сопряжено с получением несанкционированного доступа к компьютерной системе.

При этом подобные преступления совершаются не путем обмана или злоупотребления доверием конкретного субъекта, а путем тайного получения доступа к компьютерной системе и совершения тайных действий, которые в результате приводят к хищению чужого имущества или приобретению права на чужое имущество. Налицо проявление признаков статьи 158 УК РФ «Кража», то есть тайное хищение чужого имущества.

В то же время хищение с помощью компьютерных технологий (ст. 159.6), как известно, не содержит всех необходимых признаков состава кражи. Отметим также, что под хищением в УК РФ понимаются совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившие ущерб собственнику или иному владельцу этого имущества.

Вывод: хищение в сфере компьютерной информации, по существу, не укладывается в рамки только состава мошенничества или кражи, а является деянием, различные элементы, квалифицирующие признаки которого нашли отражение и в ст. 158, и в ст. 159 УК РФ. При этом напомним, что в диспозиции статьи 159.6 УК РФ в качестве способов совершения такого преступления указаны не обман и злоупотребление доверием, а ввод,

удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Как свидетельствует цитируемая редакция диспозиции названной статьи, в ней применяется терминология составов преступлений, предусмотренных ст. ст. 272 - 274 УК РФ, а не ст. ст. 158 и 159 УК РФ.

До появления в уголовном законодательстве состава мошенничества в сфере компьютерной информации в Постановлении Пленума Верховного Суда РФ от 27 декабря 2007 г. № 51 «О судебной практике по делам о мошенничестве, присвоении и растрате» было предложено подобные виды преступлений квалифицировать с учетом обстоятельств по совокупности ст. ст. 159, 272, 273 УК РФ.

Одной из целей введения в УК РФ ст. 159.6 является формирование единообразного подхода к трактовке правовой сущности понятия «обман потерпевшего». Поскольку понятие «обман» основывается на субъективной оценке, то позиции потерпевшего законом было придано правоустанавливающее значение. Вместе с тем различия в понимании сути мошенничества, основанные на видах его проявления, приводят в процессе правоприменения ст. 159.6 УК РФ к существенным трудностям. По обоснованному мнению В.И. Гладких, правоприменительная практика по делам о преступлениях, предусматривающих ответственность за компьютерное мошенничество, крайне скудна и не способствует разрешению проблемы борьбы с рассматриваемыми преступлениями, поскольку сложно установить наличие в совершенных деяниях всех признаков состава того или иного преступления, в первую очередь субъекта преступления (в силу его анонимности, объективной стороны деяния - по причине его виртуального характера; субъективной стороны - по причине сложности установления формы вины, мотива и цели) .

Для разрешения существующей проблемы необходимо сопряжение усилий сотрудников правоохранительных органов, экспертов в области уголовного права, компьютерных технологий.

Подобные проблемы отмечаются и в части, касающейся правоприменения ст. 159.3 УК РФ. Состав преступления включает в себя мошенничество с использованием платежных карт, то есть хищение чужого имущества, совершенное с использованием поддельной или принадлежащей другому лицу кредитной, расчетной или иной платежной карты путем обмана уполномоченного работника кредитной, торговой или иной организации.

Анализ различных составов преступлений на предмет установления жесткости или мягкости уголовного наказания показывает, что при наличии одновременно признаков состава преступления с отягчающими и смягчающими обстоятельствами по правилам квалификации преступлений предпочтение отдается норме со смягчающими обстоятельствами. В этой связи отметим, что мошенничество в крупном и особо крупном размере, совершенное с использованием пластиковых карт, по степени общественной опасности вряд ли чем-то отличается от обычного мошенничества.

Вместе с тем содержание и конструкция ст. 159.6 УК РФ определяют данное деяние как менее общественно опасное, нежели аналогичное завладение чужим имуществом путем обмана или злоупотребления доверием (ст. 159 УК РФ). Приведем в этой связи пример: если лицо путем обмана похитило имущество стоимостью, скажем, 1,1 млн. руб. с использованием платежных карт, то это деяние подпадает под признаки ч. 1 ст. 159.3 УК РФ (преступление небольшой тяжести) и не влечет наказания, связанного с лишением свободы. Если же имущество такой же стоимости изъято у собственника без использования платежных карт, то оно относится к числу тяжких преступлений и влечет уголовное наказание в виде лишения свободы на срок до 10 лет.

Такой полярно дифференцированный подход законодателя, мягко говоря, вряд ли логичен. Кроме того, на практике он не может проявлять себя

в качестве реального инструмента предупреждения хищений в особо крупных размерах. Ибо по факту получается, что сами составы преступлений, предусмотренные, скажем, ст. ст. 159.3 и 159.6 УК РФ, как таковые фактически выступают в роли смягчающих обстоятельств по отношению к составу преступления, установленному в ст. 159 УК РФ.

Вместе с тем, учитывая, что как основной, так и специальные составы мошенничества объединены по родовому признаку (свойству) и являются видом и подвидом хищения, то и подходы к определению признаков таких деяний и установлению уголовного наказания за такие преступления, считаем, должны быть единообразными.

Решение проблем грамотного правового регулирования усложняющихся и возникающих новых криминализированных общественных отношений возможно только на основе всестороннего анализа складывающейся ситуации в сфере борьбы с киберпреступностью, адекватно-комплексного подхода к определению путей их решения. Без проведения такой работы предпринимаемые законотворческие шаги, даже самые активные, будут и в дальнейшем способствовать включению в уголовное законодательство норм (отдельных новых статей), применение которых на практике не будет востребовано. К тому же их количество не перерастет в качество и, следовательно, не обеспечит создание реального правового механизма по активному противодействию киберпреступности.

Заключение

Проведя настоящее исследование, нами были достигнуты следующие задачи: исследовано понятие «компьютерная информация»; проанализировано законодательство Российской Федерации об уголовной ответственности за преступления в сфере компьютерной информации; рассмотрены вопросы отграничения неправомерного доступа к компьютерной информации от смежных составов преступлений; проанализированы способы совершения преступлений в сфере компьютерной информации; проанализированы проблемы и возможные пути решения в области уголовной ответственности за преступления в сфере компьютерной информации.

Проведя настоящее исследование, можно сделать следующие выводы.

На современном этапе развития общественного отношения большую роль набирают информационные технологии, так как проникают во все сферы общественной жизни. В результате этого появилась необходимость осмысления последствий их создания и практического использования. Особую роль приобретает обеспечение информационной безопасности, пронизывая все сферы человеческой деятельности.

Для уголовно-правовой характеристики преступлений в сфере компьютерной информации важно закрепление самого понятия «компьютерная информация», что и сделал российский законодатель в Примечании 1 ст. 272 УК РФ. Закрепление указанного понятия на законодательном уровне играет важную роль в уголовно-правовом аспекте.

Наименее малоизучен вопрос, затрагивающий категорию «неправомерного доступа к компьютерной информации», в то же время — это достаточно опасные преступления на современном этапе, так как приобретает наиболее угрожающие масштабы.

Для обозначения признаков неправомерного доступа к компьютерной информации и отграничения его от смежных преступлений необходимо

пользоваться методом юридического анализа. Особого внимания заслуживает вопрос об отграничении неправомерного доступа к компьютерной информации от создания, использования и распространения вредоносных компьютерных программ.

При квалификации неправомерного доступа к компьютерной информации возникает ряд вопросов, касающихся отграничения данного преступления от иных видов преступных посягательств, не только, закрепленных в главе 28 УК РФ, но и таких как: «нарушение авторских и смежных прав (ст. 146 УК РФ); «Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну» (ст. 183 УК РФ) и др.

Решение проблем грамотного правового регулирования усложняющихся и возникающих новых криминализированных общественных отношений возможно только на основе всестороннего анализа складывающейся ситуации в сфере борьбы с киберпреступностью, адекватно-комплексного подхода к определению путей их решения. Без проведения такой работы предпринимаемые законотворческие шаги, даже самые активные, будут и в дальнейшем способствовать включению в уголовное законодательство норм (отдельных новых статей), применение которых на практике не будет востребовано. К тому же их количество не перерастет в качество и, следовательно, не обеспечит создание реального правового механизма по активному противодействию киберпреступности.

Список используемой литературы

Нормативно-правовые акты

1. Конвенция о преступности в сфере компьютерной информации (ETS № 185): заключена в г.Будапеште 23.11.2001 // доступ из справ. -правовой системы «КонсультантПлюс».
2. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 (с учетом поправок, внесенных законами РФ о поправках к Конституции РФ от 30.12.2008 № 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 21.07.2014 № 11-ФКЗ) // СЗ РФ. 04.08.2014. № 31. Ст. 4398.
3. Федеральный закон «О государственной тайне»: Закон РФ от 21.07.1993 № 5485-1 (ред. от 08.03.2015) // СЗ РФ. 13.10.1997. № 41. Стр. 8220 – 8235.
4. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 30.03.2016) // СЗ РФ. 1996. № 25. Ст. 2954.
5. Указ Президента РФ от 30.11.1995 № 1203 «Об утверждении Перечня сведений, отнесенных к государственной тайне» // СЗ РФ. 04.12.1995. № 49. Ст. 4775.
6. Постановление ВС РФ от 23.09.1992 N 3524-1 «О порядке введения в действие Закона Российской Федерации «О правовой охране программ для электронных вычислительных машин и баз данных» // Ведомости СНД РФ и ВС РФ. 22.10.1992. № 42. Ст. 2326. Утратил силу.

Научная литература

7. Абов А.И. Преступления в сфере компьютерной информации: неправомерный доступ к компьютерной информации. М.: Прима-Пресс, 2002.
8. Абов А.И., Велиев Э.Э., Ткаченко С.Н. Экономическая безопасность и компьютерные преступления. М.: Прима-Пресс, 2003.
9. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. канд. ... юрид. наук. Ижевск, 2002.
10. Горшенков Г.Н. К понятию «информационная преступность» // Российский криминологический взгляд. 2005. № 4.
11. Доржиев А.В. Уголовно-правовые меры противодействия преступлениям, совершаемым в предпринимательской сфере: Дис. ... канд. юрид. наук. М., 2010.
12. Кесареева Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: Автореф. дис. ... канд. юрид. наук. М., 2002.
13. Крылов В.В. Расследование преступлений в сфере информации. М., 1998.
14. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: Дис. ... д-ра юрид. наук. М., 2006.
15. Осипенко А.Л. Борьба с преступностью в глобальных компьютерных сетях: международный опыт: Монография. М.: Норма, 2004.
16. Расследование неправомерного доступа к компьютерной информации: Учебное пособие. Изд-е 2-е, доп. и перераб. / Под ред. д.ю.н., проф. Н.Г. Шурухнова. М.: Московский университет МВД России, 2004.
17. Суслопаров А.В. Информационные преступления: Автореф. дис. ... канд. юрид. наук. Красноярск, 2008.

18. Третьяков А.Н. Криминологическая характеристика и предупреждение преступности в информационной сфере уголовно-исполнительной системы: Дис. ... канд. юрид. наук. Рязань, 2004.
19. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. ... канд. юрид. наук. Владивосток, 2005.
20. Числин В.П. Информация как объект уголовно-правовой защиты. М., 2004.
21. Широков В.А., Беспалова Е.В. Киберпреступность: история уголовно-правового противодействия // Информационное право. 2006. № 4.
22. Щепетильников В.Н. Уголовно-правовая охрана электронной информации: Автореф. дис. ... канд. юрид. наук. Елец, 2006.

Материалы юридической практики

23. Приговор Чановского районного суда Новосибирской области от 26.10.2015 по делу № 1-106/2015 // Росправосудие: [сайт]. URL: https://rospravosudie.com/court-chanovskij-rajonnyj-sud-novosibirskaya-oblast-s/act-500159171 (дата обращения: 10.04.2016).
24. Приговор мирового судьи судебного участка № 13 Кировского района г.Перми от 07.12.2015 по делу № 1-103/2015// Росправосудие: [сайт]. URL: https://rospravosudie.com/court-sudebnyj-uchastok-13-kirovskogo-rajona-g-permi-s/act-225265116/ (дата обращения: 10.04.2016).