МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ 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))

БАКАЛАВРСКАЯ РАБОТА

на тему Уголовная ответственность за преступления в сфере компьютерной информации

Студент(ка) А.Ж. Бердинов _____
(И.О. Фамилия) (личная подпись)

Руководитель В.М. Корнуков _____
(И.О. Фамилия) (личная подпись)

Допустить к защите

Заместитель ректора – директор института права
к.ю.н., доцент С.И. Вершинина_____
(ученая степень, звание, И.О. Фамилия) (личная подпись)
«_____»_____20_____г.

Тольятти 2018

Аннотация

Развитие современных информационных технологий и сети Интернет делает информацию, выложенную на различных информационных ресурсах, все более общедоступной. В связи с этим, выявление проблем, связанных с преступлениями в сфере компьютерной информации, а также совершенствование законодательства в данной области, – представляются актуальными задачами.

Итак, целью данного исследования является анализ применения уголовной ответственности за преступления в сфере компьютерной информации. Для достижения поставленной цели необходимо выполнить следующие задачи:

- дать понятие компьютерной информации как объект преступления;

- определить правовое регулирование отношений в области компьютерной информации;

- изучить принципы ответственности в системе преступлений в сфере компьютерной информации;

- охарактеризовать объект и предмет, объективные и субъективные признаки преступлений;

- дать оценку способов совершения мошенничества в сфере компьютерной информации;

- определить проблемы квалификации преступлений в сфере компьютерной информации со смежными составами и предложить способы их профилактики.

Объем работы – 53 страницы. Структура работы состоит из введения, 2 глав, 6 параграфов, заключения и списка используемых источников.

Содержание

Введение…….4

1. Понятие компьютерной информации и ее правовое регулирование...7

1.1 Компьютерная информация как объект преступления……...7

1.2 Правовое регулирование отношений в области компьютерной информации……12

1.3 Ответственность в системе преступлений в сфере компьютерной информации……16

2. Характеристика преступлений в сфере компьютерной информации для назначения уголовной ответственности……...20

2.1 Объект и предмет, объективные и субъективные признаки преступлений…….20

2.2 Оценка способов совершения мошенничества в сфере компьютерной информации…….24

2.3 Проблемы квалификации преступлений в сфере компьютерной информации со смежными составами и их предупреждение……...34

Заключение……..46

Список используемых источников...…….49

Введение

Развитие современных информационных технологий и сети Интернет делает информацию, выложенную на различных информационных ресурсах, все более общедоступной. Такая общедоступность дала простор для развития преступных направлений в данной области. Ежемесячная аудитория интернет-пространства в рамках Российской Федерации к весне 2017 года достигла 87 миллионов человек, что составляет 71% от всего населения страны[1]. В связи с этим, выявление проблем, связанных с преступлениями в сфере компьютерной информации, а также совершенствование законодательства в данной области, – представляются актуальными задачами.

Следует обозначить, что ответственность за преступления в сфере компьютерной информации российский законодатель регламентировал в положениях главы 28 Уголовного кодекса Российской Федерации, которая включила в свой состав всего три статьи: «Неправомерный доступ к компьютерной информации», «Создание, использование и распространение вредоносных компьютерных программ» и «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей»[2].

Иных норм, которые предусматривали бы ответственность за незаконные действия в сфере компьютерной информации российское законодательство не содержит.

Очевидно, что при таком небольшом объёме правового регламентирования в представленной области большой пласт вопросов остался без должного внимания.

---

[1] Количество пользователей интернета в России // Интернет в России и в мире [Электронный ресурс]. – Режим доступа: http://www.bizhit.ru/index/users_count/0–151

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_10699/

Наряду с развитием информационных технологий, формируются, модифицируются и эволюционируют новые виды и формы преступлений, что, в свою очередь, проявляет прямое воздействие на понятийный аппарат и сложность квалификации преступных деяний. Итак, целью данного исследования является анализ применения уголовной ответственности за преступления в сфере компьютерной информации. Для достижения поставленной цели необходимо выполнить следующие задачи:

- дать понятие компьютерной информации как объект преступления;

- определить правовое регулирование отношений в области компьютерной информации;

- изучить принципы ответственности в системе преступлений в сфере компьютерной информации;

- охарактеризовать объект и предмет, объективные и субъективные признаки преступлений;

- дать оценку способов совершения мошенничества в сфере компьютерной информации;

- определить проблемы квалификации преступлений в сфере компьютерной информации со смежными составами и предложить способы их профилактики.

В ходе написания настоящей работы были использованы такие методы, как методы систематизации имеющихся сведений, исследования, анализа, синтеза, сравнительно-правовой, логический, статистический, исторический, конкретно социологический, то есть совокупность общенаучных и частных методов исследования, а также осуществлялся анализ нормативных правовых актов, юридической литературы, обобщение полученных данных.

В качестве теоретической основы выступили труды известных ученных правоведов таких, как О.Я. Баев, В.А. Мещеряков, Е.А. Лысак, В.С. Минская, А.А. Нагорный, С.А. Смолин, Н.А. Чуриков и многих других.

В качестве нормативно-правовой базы использовались положения Конституции Российской Федерации, федеральные законы и нормативно-правовые акты, действующих в настоящее время в рассматриваемой области.

Структура работы состоит из введения, 2 глав, 6 параграфов, заключения и списка используемых источников.

1. Понятие компьютерной информации и ее правовое регулирование

1.1 Компьютерная информация как объект преступления

Сфера компьютерной информации, как любая другая сфера человеческой деятельности, подвержена преступлениям, за совершение которых предусмотрена уголовная ответственность, зафиксированная в статьях 272, 273 и 274 УК. В связи с интенсивным развитием информационных технологий указанные статьи требуют определенных изменений, что и было сделано в Федеральном законе от 7 декабря 2011 г. N 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации». Внесенные новым законом изменения вызывают профессиональный интерес у специалистов, комментирующих новую редакцию всех трех статей 272, 273 и 274 УК, в которых установлена уголовная ответственность за совершенные преступления, каким может быть подвергнута сфера компьютерной информации[3].

Законодатель в новой редакции статей 272, 273 и 274 УК устанавливает объединяющий общий для всех трех составов объект преступления в виде общественных отношений, связанных с посягательством на компьютерную информацию. Особенности объекта преступления в совершенных компьютерных преступлениях вызывают определенный научный интерес. В связи с этим можно привести слова А. Пионтковского: «объект преступления есть тот необходимый признак состава каждого преступления, который в значительной мере определяет природу данного преступления и степень его общественной опасности»[4].

---

[3] Быков В.М., Черкасов В.Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. N 5. С. 15.

[4] Пионтковский А.А. Курс советского уголовного права: в шести томах / Редакционная коллегия: А.А. Пионтковский, П.С. Ромашкин, В.М. Чхиквадзе. М.: Наука, 1970. Часть общая. Том II. Преступление. С. 115.

Прежде чем рассматривать компьютерную информацию применительно к уголовному праву в качестве объекта преступления, следует определить исходное положение при правильном понимании и раскрытии этого понятия «объект преступления», которым будет само понятие «информация». Федеральный закон от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации» содержит статью 2, в которой указано, что «информация - сведения (сообщения, данные), независимо от формы их представления»[5].

Таким образом, Федеральный закон «Об информации, информационных технологиях и о защите информации», содержит полное определение «информация», а в гл. 28 УК речь идет о компьютерной информации, только как о разновидности информации[6]. Эта компьютерная информация защищается уголовным законом, в частности, об этом указано в ч. 1 ст. 272 УК. Однако конкретного указания о поставленной цели именно охранять компьютерную информацию в ст. ст. 273 и 274 УК относительно этих составов законодателем не поставлено, что вовсе не означает отсутствия функции охраны. Просто законодателю нет необходимости ставить вопрос о данном положении еще два раза. Специалисты признают такое положение вещей правильным, так как защищающие компьютерную информацию нормы содержатся не только в Уголовном Кодексе.

Федеральный закон «Об информации, информационных технологиях и о защите информации» включает в себя статью 16, в первой части которой говорится о защите информации, как о указании цели, достигаемой принятыми правовыми, организационными и техническими мерами, а именно:

— защищая информацию, предотвратить неправомерный доступ, уничтожение, модифицирование, блокирование, копирование,

[5] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

[6] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

предоставление, распространение, а также иные неправомерные действия в отношении обеспечения защиты такой информации;

— соблюдать конфиденциальность информации, имеющей ограниченный доступ;

— реализовать право, разрешающее доступ к информации.

Говоря о компьютерной информации как объекте преступления, следует рассмотреть ее особенности в соответствии с новой редакцией статей 272, 273 и 274 УК.

Прежняя редакция ч. 1 ст. 272 УК фиксировала местоположение компьютерной информации, а точнее, просто информации, на машинном носителе, это может быть электронно-вычислительная машина (ЭВМ), система ЭВМ или их сеть.

Представляется более правильным подход законодателя к месту возможной дислокации охраняемой законом компьютерной информации, когда новая редакция ч. 1 ст. 272 УК не содержит перечня всех пригодных для этого технических средств.

Прогресс не остановить, электронно-вычислительная техника находится в постоянном развитии, что предопределяет создание и ввод в обращение все новых технических средств, способных содержать, использовать и хранить компьютерную информацию. В таком случае законодатель был бы обязан непрерывно реагировать на технический прогресс, изменяя уголовный закон и указывая в нем обновление носителей компьютерной информации.

Примечание 1 к ст. 272 УК в новой редакции содержит указание на вид представления компьютерной информации в форме электрических сигналов без конкретизации средств, способных их хранить, обрабатывать и передавать. Особые возражения по такому определению компьютерной информации не возникают, хотя и упрощать это понятие не стоит.

Представляется необходимым дополнительно разъяснить понятие «компьютерной информации». Нередко общественное сознание, да и

законодательство, рассматривают информацию только как совокупность неких сведений или данных, хотя в реальности данное определение звучит не совсем так. Считая существование сведений событием объективным, следует пояснить, что информацию компилирует только субъект, анализирующий и сопоставляющий эти сведения вкупе со своими знаниями об этом объекте, в результате субъект использует все это при принятии управленческих решений. Для науки кажущаяся простота понятия «информация» не является достаточно ясной. Учитывая сказанное, использование законодателем термина «компьютерная информация» в статьях 272, 273 и 274 УК с целью обозначить объект преступления, представляется не совсем точным, вследствие чего сама наука уголовного права является источником спорных предложений.

Рассматривая компьютерную информацию как объект преступления, следует отметить существование ее особенностей, одна из которых заключается в невозможности ее существования «самой по себе», то есть без конкретного носителя, она не может быть отделима от технических средств. В настоящее время существует множество различных технических средств, и это не обязательно будет только компьютер. Компьютером в широком смысле слова можно назвать и современный мобильный телефон, и банкомат, и пр.

Для того, чтобы законодателем вышеуказанные устройства рассматривались в качестве объекта компьютерного преступления, а статьи УК имели возможность защитить информацию, которую содержат эти технические средства, по подобию компьютерной информации, следует дать определение понятию «компьютер». Прежде всего, это устройство, способное выполнять четко заданный алгоритм выполнения последовательности операций, чаще всего представляющий численные расчеты и манипулирование данными. Резюмируя вышесказанное, можно сказать, что объектом преступления, указанным в гл. 28 УК, следует считать любую информацию, которую содержат любые технические средства.

Невозможно не заметить толкование новым уголовным законом классического понятия информации и «компьютерной информации», оно не совсем совпадает с определением информации, данном наукой об управлении - кибернетикой - (имеющий самый упрощенный вид), нечто необходимое для субъекта управления, принимающего оптимальное решение при воздействии на управляемый объект.

Принимая во внимание определение информации кибернетикой, можно представить ее в виде синтеза трех элементов:

1) субъект определяет для себя главную цель;

2) суммирование сведений и /данных, характеризующих состояние объекта;

3) наличие определенного состава знаний субъекта, позволяющего оценить эти сведения.

Кроме того, начиная с середины прошлого века, в данный синтез встраивается четвертый элемент информации в виде математического аппарата, оптимизирующего процесс принятия решений.

Как уже отмечалось, информацию нельзя отделить от носителя, невозможно ее существование «само по себе», еще сложнее представить природу отчуждения информации от компьютерного носителя. Необходимо связать понятие «информация» и процесс хищения, традиционно применяющийся к материальным объектам. Информация, принадлежащая собственнику (или владельцу), независимо от того, что была украдена (скопирована), остается у него. Компьютерная информация не включает в себя понятие «подлинник-копия», обычно применяемое к «бумажным» носителям в качестве важного признака при квалификации правонарушения[7].

Определенная сложность заключается и в определении цены (стоимости) рассматриваемого объекта. Как известно, любой материальный объект характеризуется тесно связанными между собой ценой производства

[7] Черкасов В.Н. Дискретность интеллектуальной собственности, или С чего начинается копия? // Защита информации. Инсайт. 2011. N 2(38). С.12.

и потребительской стоимостью. К информации же возможно применить лишь стоимость потребительскую, так как данную стоимость определяет сам субъект. «Компьютерная информация» – это весьма специфичный объект права именно в связи с перечисленными и некоторыми другими особенностями (например, с недостаточно разработанными этическими нормами в информационной сфере).

При исследовании объекта компьютерного преступления следует учесть и такую особенность компьютерной информации, когда в данном процессе юристы не могут полностью использовать привычные для них понятия. Например, они не могут полностью воспользоваться традиционным юридическим термином «кража» в отношении компьютерной информации, так как даже если информация из компьютера украдена, для владельца она не потеряна, оставаясь доступной для собственного пользования. Кроме того, юристы не могут использовать в качестве важного признака при квалификации некоторых преступлений такие привычные понятия, как копия документа и его подлинник.

Именно такими необычными свойствами компьютерной информации объясняется сложность правовой квалификации преступлений, совершаемых по отношению к такому объекту, как компьютерная информация.

1.2 Правовое регулирование отношений в области компьютерной информации

Правовое регулирование отношений в области компьютерной информации осуществляется с помощью следующих нормативно-правовых актов.

ФЗ РФ «Об информации, информационных технологиях и о защите информации»[8]. Усовершенствование законодательства по развитию и применению информационных потенциалов и возможностей в процессе внедрения современных технологий во все сферы деятельности человека, особенно в промышленности, науки, в области управления, в медицине – это основополагающее направление федеральной нормы права. Область влияния закона относится к отношениям, появляющимся при использовании своих законных прав, когда отыскивают, получают, распространяют информацию, а также при использовании компьютерных технологий, обеспечивают защиту сведениям (статья 1).

Законом прописаны правила управления государством в области пользования компьютерных технологий (статья 12), информационных коммуникационных систем (статья 15) и по защите информационных сведений (статья 16), соответственно законом определены обязательства при нарушении права в этих областях (статья 17).

Законом России «О средствах массовой информации» статьей 1 указано, что свободное распространение информации общего пользования не ограничивается, кроме фактов, указанных законом о массовой информации[9]. Не ограничиваются действия по поиску, получению, передачи сведений массового назначения, не ограничивается деятельность образования, владения средствами по распространению информации массового назначения. Не относится к числу ограничений создание, получение, сохранение и использование технического обустройства, сырьевых и материальных составляющих по производству и распространению продуктов информатизации общества.

Законом Российской Федерации «О государственной тайне» определяются положения по соотнесению информации в раздел по охране

[8] Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

[9] Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» (ред. от 18.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_1511/

государственных тайн, обеспечивающих безопасность страны, снятие грифа секретности с некоторых данных[10]. Положениями данной правовой нормы рассматриваются действия по охране информации, имеющие отношения к государственной тайне. Этот законодательный акт сохраняет правопреемство в вопросах сохранности большей части информации, относящейся к нормативной документации, обеспечивает защищенность сведений на протяжении всего срока фактического сосуществования. Основой замысла данной правовой нормы служит положение о переориентировании имеющейся структуры по обеспечению безопасности информационных сведений на создание сбалансированности государственных, личностных, общественных значимостей во всех областях жизнедеятельности человека (экономика, политика, управление и пр.), обеспечить развитие и реализацию отношений в области права.

Законом Российской Федерации «О связи» определяются положения правоотношений в деятельности служб коммуникаций (связь), в функционировании которых принимают участие государственные структуры, операторы коммуникаций, те, кто пользуется связью, а также ряд должностных лиц[11]. Данной нормой закона определяется деятельность в сфере средств связи, правомочия в этой сфере принадлежат государственным структурам – федеральной связи, которая координирует правовые отношения, полномочия, круг обязанностей для всех субъектов, которые принимают участие по обеспечению услуг коммуникаций (связь).

Гражданский кодекс Российской Федерации в части 1 и части 2 представляет информацию в качестве объекта гражданских норм закона, также, как и интеллектуальную собственность или имущество (статья 128). Кодекс дает трактовку сведениям, которые относятся к коммерческой или служебной тайне. Статья 139 предоставляет формальные особые составы

[10] Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (ред. от 26.07.2017) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

[11] Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ (ред. от 18.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/

правонарушений, на основании которых применяют меры воздействия при нарушении секретности сведений[12].

Права на обладание информацией, гарантирование защиты информации, а также разделение областей деятельности в информатизации общества отражены Конституцией Российской Федерации и в Гражданском кодексе.

Уголовным кодексом определяются направления решения части проблем по уголовному праву. Главой 28 «Преступления в сфере компьютерной информации» квалифицированы преступления в разделе использования компьютерной техники в информатизации процессов, которые представляют общественную опасность.

Уголовным кодексом квалифицированы преступления, угрожающие конституционным правам и свободам граждан, имеющим информационную направленность[13]:

- несоблюдение секретности переписок, разговоров по телефонной связи, телеграфного или другого сведения (часть 1 статьи 138);

- противозаконное изготовление, распространение, получение с целью сбыта спецсредств технического назначения, необходимых для скрытной добычи сведений (часть 3 статьи 138);

- передача от официального лица любому другому лицу информации не в полном объеме, фактически неверных сведений и этим наносится вредное воздействие законному праву гражданина (часть 3 статьи 140);

-противоправное применение чужого объекта авторского права, приписывание чужого авторства (часть 1 статьи 146);

- несоблюдение авторского права, которое совершила группа граждан (часть 2 статьи 146);

---

[12] Гражданский кодекс Российской Федерации часть 4 18 декабря 2006 года N 230-ФЗ (ред. от 01.07.2017) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_64629/

[13] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

- противозаконное применение открытия, производственных образцов, распространение информации и сути изобретенного объекта без наличия авторского соглашения либо до официального опубликования информации по изобретению, использование чужого авторства, принудительное вхождение в соавторство (часть 2 статьи 147);

- отображение в рекламных проспектах сведений содержащих заведомую ложь по товарам, услугам, производителям (часть 1 статьи 182);

- сбор информации, относящейся к банковской, коммерческой тайне, похищая документацию, подкупая, угрожая либо применяя другие незаконные методы (часть 1 статьи 183);

- противозаконное применение или распространение информации, содержащей сведения по банковской либо коммерческой тайне и, не обладая согласием владельцев (часть 2 статьи 183);

- противозаконная продажа за рубеж сведений научной, технической, технологической направленности, относящихся к военно-техническому комплексу (часть 2 статьи 189).

1.3 Ответственность в системе преступлений в сфере компьютерной информации

Уголовный кодекс выделяет преступления в сфере компьютерной информации как отдельный вид правонарушений по нескольким причинам. Во-первых, в качестве объекта преступления выступает компьютерная информация – и потому различаются как состав преступлений, так и меры наказания, последующие за ними. Во-вторых, рассматриваемые в статье правонарушения значительно участились за последние годы, что было связано с переходом предприятий на автоматизированное производство.

1. Неправомерный доступ к информации.

В Российский Федеральный Закон под преступлениями в сфере электронной или компьютерной информации понимает уголовно наказуемую деятельность, предметом посягательства которой является компьютерная информация. В свою очередь, компьютерная информация – это сведения, находящиеся на физическом носителе или данные, которые могут быть переданы по каналам телекоммуникации в форме машинного кода, доступного для чтения с помощью ЭВМ. Субъект посягательств – дееспособное лицо старше 16 лет (на момент совершения преступления).

Статья 274 предусматривает наличие у данного лица доступа к защищаемой компьютерной информации по служебному положению. В качестве предмета преступления выступает компьютерная информация, временно или постоянно располагаемая в памяти ЭВМ или на иных физических носителях. В результате неправомерного доступа часть информации или вся она целиком может быть скопирована, изменена или модифицирована, а также удалена с носителя. Копирование не предусматривает изменение первоначального источника, а лишь воспроизведение некой информации в корыстных целях. Модификация – изменения, вводимые пользователем или группой пользователей без цели обеспечить бесперебойное функционирование ЭВМ или их систем. Под удалением информации подразумевают частичное или полное уничтожение ее в результате стирания с носителей. Человек, совершающий преступление, может являться как абсолютно посторонним лицом, так и сотрудником организации, уже имеющим доступ к информации, соответствующий его служебному положению.

2. Разработка и распространение вредоносного ПО.

Данный вид правонарушения выражается в одном или нескольких следующих действиях:

— проектирование и разработка программного обеспечения для ЭВМ, действие которого направлено на удаление, блокирование, изменение или

копирование информации, а также на провоцирование сбоев в работе ЭВМ или их систем/сетей;

— модификация описанного выше программного обеспечения;

— непосредственное использование описанного выше программного обеспечения или физических носителей с данным ПО;

— распространение (как умышленное, так и непроизвольное) описанного выше программного обеспечения.

3. Неправильная эксплуатация ЭВМ и их систем.

Нарушение правил использования ЭВМ, систем или сетей подразумевает последующее за этим стирание информации, либо ее блокирование/модификацию. Объект преступления – это охраняемая законодательством информация, доступ к которой имеет только строго ограниченный круг людей. Состав преступления рассматривается даже в том случае, если оно было совершено по неосторожности, но повлекло за собой тяжкие последствия. В зависимости от того, было ли неправильное использование случайным или намеренным, меры наказания за совершенное правонарушение несколько отличаются.

УК РФ предусматривает наказание за рассматриваемые преступления по 3 статьям.

Согласно статье 272 УК РФ «Неправомерный доступ» предусматривается одно из следующих наказаний:

- штраф, составляющий 200-500 минимальных размеров оплаты труда/доходов преступника за 2-5 месяцев;

- исправительный труд – от полугода до года;

- ограничение свободы – до 2 лет.

Если преступление совершила группа лиц по сговору либо служебное лицо, имеющее доступ к важной информации, предусматриваются иные меры наказания:

- все соучастники выплачивают сумму в 500-800 минимальных зарплат или других доходов за 5-8 месяцев;

- каждый проговаривается к обязательным работам – от года до 2 лет; арест – 3-6 месяцев;

- тюремное заключение – до 5 лет.

Статья 273 УК РФ «Разработка, эксплуатация и распространение вирусных программ» предполагает следующее наказание:

- лишение свободы – до 3 лет + выплаты 200-500 мин. размеров оплаты труда/доходов правонарушителей за 2-5 месяцев;

- 3-7 лет тюремного заключения (при преступлениях, имевших тяжкие последствия).

Статья 274 УК РФ «Неправильное использование ЭВМ и их систем» предусматривает следующие меры наказания:

- лишение возможности занимать некоторые конкретные должности (обычно в госорганах) до 5 лет; обязательные работы – 180-240 часов;

- лишение права выезда с определенной территории – до 2 лет;

- тюремное заключение до 4 лет (при правонарушениях, имевших тяжкие последствия).

Поскольку компьютерная информация не является материальным предметом, иногда бывает достаточно сложно не только определить состав преступления при ее хищении, но и непосредственно это хищение зафиксировать. Большому проценту ненаказуемости подобных преступлений способствует и компьютерная неграмотность населения – из-за этой огласки и вынесению дела в суд предаются только особо громкие случаи, повлекшие за собой сбой в работе крупных организаций.

В России глава УК, соответствующая компьютерным преступлениям, была разработана и принята только в 1997 году. По сравнению с западными коллегами, ведущими дела в этой сфере уже с 70-х годов, у нас еще не накоплен достаточный опыт, позволяющий компетентно рассматривать данные правонарушения. Более того, в российском законодательстве пока еще нет документов, которые могли бы регламентировать компьютерные доказательства.

2. Характеристика преступлений в сфере компьютерной информации для назначения уголовной ответственности

2.1 Объект и предмет, объективные и субъективные признаки преступлений

Под такими преступлениями понимают преступления причинения ущерба, нанесение вреда умышленными действиями (бездействиями) или создавшие опасность общественному порядку, регулирующим защищенное создание, сохранение, применение, передачу информационных сообщений.

Первый раз законодательство России квалифицировало подобные противоправные деяния в Уголовном кодексе от 1996 года. Глава 28 содержит ряд статей о несении обязательств за преступные действия в области компьютерных информационных сообщений:

- статья 272 Уголовного кодекса - за незаконный доступ компьютерному информационному сообщению;

- статья 273 - за производство, применение, передачу, рассылку программ для компьютерной техники, имеющей вредоносное действие;

- статья 274 - за уклонение от установленных норм использования способов сохранения, переработки и распространения компьютерных сообщений с применением сетей телекоммуникации[14].

В качестве родового объекта таких преступных действий считается безопасность общественных отношений (гл. 28).

В качестве видового объекта – защищенность в области применения компьютерных информационных сообщений, т.е. область общественных отношений, которой обеспечена надежная защита по использованию компьютерной техники, компьютерной телекоммуникационной сети, в

[14] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/ cons_doc_LAW_10699/

которой исключается нанесение вредного воздействия на личность, либо общество, либо государство.

К непосредственным объектам преступных деяний в области использования компьютерных информационных сообщений относят некоторые разновидности отношения, которые относятся к содержанию указанного вида защищенности, такие как неприкосновенное содержание информации в компьютере, в компьютерных сетях, правильность использования систем, невозможность нанесения вредоносного воздействия на личность, общество, государство.

В качестве предмета в области компьютерного противоправного деяния считается информация, которая охраняется законом (статьи 272, 274 Уголовного кодекса Российской Федерации).

Объективной стороной таких преступлений считается действия (бездействия), имеющих отношение к использованию компьютерной системы или сети и нанесшие вредное воздействие на личность, общество, государство либо имеющее намерение совершить вредоносное воздействие.

Субъективную сторону подобных преступных действий определяет наличие вины с умышленным воздействием или по неосторожности. Ряд составов преступных деяний предполагают наличие вины только по неосторожности.

Статья 272 Уголовного кодекса в части 1 оговаривает меру ответственности за незаконное проникновение к информационным сообщениям, содержащимся в компьютере и которые охраняются нормами закона, при условии, что эти действия привели к потере информации, её блокировке, несанкционированному копированию.

Объектом преступного деяния будет защищенность компьютерной информации в деятельности собственника, законного владельца, пользователя компьютерных коммуникационных сетей при сборе, переработке, накапливании, сохранении, употреблении информационных сообщений.

Предметом преступного деяния будет информация, содержащаяся в компьютере или в информационной системе и имеющая отношение к личности, фактам, событиям, деятельности. Так же к предмету преступного деяния относится и само компьютерное устройство, в качестве носителя информации и в данной ситуации оно не оценивается в качестве вещи или устройства, обладающее конкретной денежной оценкой.

Объективную сторону преступного деяния определяют:

1) поступки, т.е. незаконное проникновение к информации, которую защищают нормы закона;

2) результаты действий (потеря информации, блокировка, трансформация (модифицирование), создание несанкционированной копии);

3) причинная взаимосвязь действий и наступивших результатов этих действий[15].

Удаление информации, т.е. её уничтожение, потеря без возможного воссоздания, осуществить ликвидацию её из компьютерной памяти либо удалить части информации, влияющие на основополагающие и характеризующие информационные признаки.

Блокировка информации, т.е. сделать неосуществимость её применения, хотя сама информация сохраняется.

Модифицирование информации, т.е. изменить содержание и суть информации по отношению к той, что имелась у владельца до вмешательства извне.

Создание несанкционированной копии, т.е. противозаконное создание копии, имеющей необходимые сведения в любом материальном виде.

Состав преступления – материальный.

К субъекту преступного деяния относят любого вменяемого гражданина, достигшего возраста шестнадцати лет.

---

[15] Быков, В.М., Черкасов, В.Н. Понятие компьютерной информации как объекта преступлений // Законность. 2013. N 12. С. 37 - 40.

Субъективную сторону подобных преступных действий определяет наличие вины с умыслом прямой или косвенной формы.

Статья 272 Уголовного кодекса России в части 2 рассматривает такое же преступление только с причинением ущерба в крупном объеме либо исполненное из корыстных целей.

Статья 272 Уголовного кодекса России в части 3 рассматривает преступления, перечисленные в частях 1, 2 и которые совершила группа граждан с предварительным сговором либо организованная группа, либо лицо, превысившее или нарушившее свои должностные компетенции.

Статья 272 Уголовного кодекса России в части 4 рассматривает преступления, указанные частями 1, 2, 3 при условии наличия тяжких последствий либо привели к угрозе их наличия.

На основании примечания:

1. компьютерная информация – это некоторый объем сообщений, данных, записанных с помощью электронных импульсом, не зависящих от способов их сохранения, способов переработки и распространения;

2. крупный ущерб (статьи из гл. 28) – это нанесение ущерба, оценивающего суммой более одного миллиона руб.

Статья 274 Уголовного кодекса в части 1 рассматривает несение обязательств:

- за несоблюдение условий использования способов сохранения, переработки, распространения компьютерных информационных сведений;

- за несоблюдение условий использования компьютерных информационных систем;

- за несоблюдение требований по использованию компьютерных коммуникационных систем, приведших к ликвидации, блокировке, модифицированию информации, или создание несанкционированных копий и нанесение, тем самым, ущерба в крупном объеме.

В качестве непосредственного объекта преступного деяния выступают общественные отношения, гарантирующие безопасное и правильное

использование возможностей сохранения, переработки, распространения компьютерных сведений и компьютерных коммуникационных систем.

Предметом преступного деяния являются компьютерные сведения, которые охраняют нормы закона.

Объективную сторону преступного деяния определяют:

1) поступки (действие, бездействие) - несоблюдение требований использования возможностей сохранения, переработки, распространения компьютерных сведений, находящихся под охраной, информационных коммуникационных систем и требований доступа к ним, приведшие к ликвидации, блокировке, трансформации или копированию сведений;

2) результаты действий (последствия) – нанесение ущерба в крупном объеме;

3) причинная взаимосвязь действий и наступивших результатов этих действий[16].

Состав преступления – материальный.

К субъекту преступного деяния относят любого вменяемого гражданина, достигшего возраста шестнадцати лет, который имеет возможности доступа к компьютерным сетям.

Субъективную сторону подобных преступных действий определяет наличие вины с умышленным воздействием или по неосторожности.

Статья 274 Уголовного кодекса в части 2 рассматривает несение обязательств за такие же преступления, приведшие к тяжким последствиям либо обеспечившие наличие угрозы таких последствий.

2.2 Оценка способов совершения мошенничества в сфере компьютерной информации

[16] Смолин, С.А. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений. – М.: Юрайт, 2016. – 201 с.

Общепризнано, что правосудие призвано обеспечить достаточный уровень защищенности человека, общества и государства, что предполагает выполнение последним его функций правоохраны[17]. Именно на это в конечном итоге направлены изменения и дополнения уголовного законодательства, среди которых значительный интерес в научной литературе вызывает систематизация преступных деяний в сфере мошенничества.

Так, введение специальной уголовной ответственности за мошенничество в сфере компьютерной информации было воспринято в научном мире неоднозначно. Некоторые исследователи утверждают, что описанное в ст. 159.6 УК РФ деяние не является мошенничеством[18], другие указывают на неясные и противоречивые формулировки, используемые законодателем в конструкции диспозиции статьи[19]. Изучение данных позиций обнаруживает множество дискуссионных вопросов. Вместе с тем представляется, что исследование и уяснение содержания признаков состава преступления позволят снять некоторые из них. Учитывая предмет нашего исследования, в рамках данной работы мы рассмотрим некоторые аспекты, касающиеся раскрытия сущности и содержания отдельных признаков объективной стороны мошенничества в сфере компьютерной информации.

В диспозиции ч. 1 ст. 159.6 УК РФ указано, что мошенничество в сфере компьютерной информации представляет из себя хищение чужого имущества или приобретение права на чужое имущество, что в целом соответствует определению внешнего проявления мошенничества, закрепленного в общей норме ст. 159 УК РФ. Учитывая, что проблематика исследования обязательных признаков объективной стороны мошенничества

---

[17] Звонов, А.В. Система мер уголовно-правового воздействия: сущность и содержание // Человек: преступление и наказание. 2015. N 3. С. 97.

[18] Хилюта, В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. N 3. С. 113.

[19] Ефремова, М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. N 4. С. 19.

достаточно освещена в научной литературе[20], не станем заострять на ней внимание, а остановимся на криминообразующем значении специфических признаков объективной стороны мошенничества в сфере компьютерной информации - способах и средствах совершения данного преступления.

Итак, диспозиция ч. 1 ст. 159.6 УК РФ содержит указания на следующие способы совершения мошенничества в сфере компьютерной информации: ввод, удаление, блокирование, модификация компьютерной информации и иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Исследование данных способов совершения мошенничества в сфере компьютерной информации необходимо начать с анализа средств совершения преступления. Средствами преступления являются компьютерная информация и средства хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Следует отметить, что понятие «компьютерная информация» в анализируемом составе преступления традиционно[21] воспринимается через определение, представленное в ч. 1 примечания к ст. 272 «Неправомерный доступ к компьютерной информации», где под ней понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи. Как мы видим, сущность компьютерной информации сводится к ее природе, выраженной в электрических сигналах.

Вместе с тем подобное понимание компьютерной информации как средства, позволяющего осуществить хищение имущества потерпевшего, вызывает нарекания[22]. Так, например, В.М. Быков и В.Н. Черкасов отмечают, что научно-технический прогресс в области информационных технологий

---

[20] Камышов, Д.А. Понятие и признаки мошенничества в Российском уголовном законодательстве // Проблемы в Российском законодательстве. 2012. N 2. С. 149

[21] Елин, В.М. Неправомерный доступ к компьютерной информации // Бизнес-информатика. 2013. N 2. С. 72.

[22] Там же. С.74.

привел к появлению новых способов представления информации: биотехнологический, лазерный, нанотехнологической, что ставит под сомнение отождествление понятия «компьютерная информация» с понятием «электронная информация»[23], которую, таким образом, следует рассматривать как один из видов компьютерной информации.

Аналогичной точки зрения придерживается и П.С. Яни, который предлагает под компьютерной информацией как средством совершения преступления, предусмотренного ст. 159.6 УК РФ, считать сведения, хранящиеся, обрабатываемые, принимаемые и передаваемые предназначенными для этих целей и снабженными соответствующим программным обеспечением техническими устройствами, функционирование которых основано на любых (различных) физических принципах действия[24]. Как видим, данное определение опирается на общее представлении о компьютере как техническом устройстве, деятельность которого осуществляется в рамках программного обеспечения.

Если непосредственно оценивать сущность компьютерной информации как средства мошенничества в компьютерной сфере, то в качестве ее выступают команды, вводимые с клавиатуры или с помощью звуковых сигналов, различного рода «вирусные» программы, а также иная информация, способная осуществить неправомерное воздействие на предмет хищения[25]. Например, г-н П., работая продавцом в магазине компьютерной техники, обнаружил на мониторе служебного компьютера открытый файл обновлений программы «1С-Рарус». Поняв, что обновление данный программы «еще не осуществлено, П. с целью хищения имущества магазина изменил в открытом файле обновлений стоимость сотового телефона, снизив ее, после чего выполнил обновление программы, модифицировав программу 1С-Рарус, а затем выполнил действия продажи сотового телефона по

[23] Быков, В.М., Черкасов, В.Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. N 5. С. 16.

[24] Яни, П.С. Специальные виды мошенничества // Законность. 2015. N 8. С. 35 - 40.

[25] Хилюта, В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. N 3. С. 114.

заведомо заниженной цене»[26]. Как видим, средством преступления послужила команда, изменившая стоимость предмета преступления - сотового телефона.

Существует определенная трудность в понимании конструкции ст. 159.6 УК РФ, которая разделила совершение преступления на две группы: средства хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационные средства.

Однако не все исследователи (особенно специалисты технических специальностей) склонны к разделению данных понятий. Так, например, И.Р. Бегишев к средствам хранения, обработки или передачи компьютерной информации относит персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается[27].

В.М. Быков и В.Н. Черкасов также не проводят принципиальной разницы между средствами хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационными средствами, объединяя их общим понятием «компьютеры». При этом к компьютерам данный авторский коллектив относит мобильные телефоны, банкоматы, смартфоны, «планшетники», главное, чтобы данные устройства реализовывали функции по автоматизированному вводу, хранению, обработке и передаче данных[28].

Если при определении сущности данных объектов взять за основу положения Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», рассматривающего информационно-телекоммуникационную сеть как технологическую систему, предназначенную для передачи по линиям связи

---

[26] Уголовное дело N 1-90/2013. Архив Первомайского районного суда г. Пензы за 2013 г. [Электронный ресурс]. – Режим доступа: http://pervomaisky.pnz.sudrf.ru/modules.php? name=norm_akt&id=124

[27] Бегишев, И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УРФО. Безопасность в информационной среде. 2012. N 1. С.16.

[28] Быков, В.М., Черкасов, В.Н. Понятие компьютерной информации как объекта преступлений // Законность. 2013. N 12. С. 38.

информации, доступ к которой осуществляется с использованием средств вычислительной техники, представляется, что разница между средствами хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационными средствами заключается только в наличии технической возможности передачи информации по линиям связи. С учетом того что подавляющее число средств хранения, обработки или передачи компьютерной информации в настоящее время имеет доступ к линиям связи, полагаем, что собственно средствами хранения, обработки или передачи компьютерной информации являются карты памяти различных видов и компьютеры, не подключенные к каким-либо линиям связи (в том числе и к локальным сетям).

При совершении мошенничества в компьютерной сфере виновные осуществляют ввод, удаление, блокирование, модификацию компьютерной информации или иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Интересно отметить, что включение в диспозицию ст. 159.6 УК РФ упоминания данных способов совершения мошенничества неоднозначно воспринимается в научном мире. Так, например, И.Г. Чекунов, подчеркивая, что в ст. 159.6 УК РФ в качестве способов совершения преступления указаны не обман и злоупотребление доверием (что отражает природу хищения), а ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации, приходит к выводу, что деяние, предусмотренное данной нормой, представляет из себя самостоятельный вид хищения[29]. Позволим себе не согласиться с данной точкой зрения. Во-первых, следует отметить, что законодатель, конструируя указанную норму, использовал общее понятие «мошенничество», которое исходя из диспозиции родовой нормы (ст. 159 УК

[29] Чекунов, И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества // Российский следователь. 2015. N 17. С.30.

РФ) представляет из себя хищение, совершенное путем обмана и (или) злоупотреблением доверием, что, безусловно, подразумевает их присутствие и в специальной норме ст. 159.6 УК РФ. Представляется, что законодатель отказался от упоминания их, чтобы не перегружать норму. Во-вторых, если соотнести обман и злоупотребление доверием с другими способами совершения мошенничества в компьютерной сфере, специально указанными в диспозиции ст. 159.6 УК РФ, становится очевидно, что первые следует рассматривать в качестве основных способов совершения преступления, в рамках которых реализуются ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство, которые следует воспринимать как специальные способы совершения преступления. Специальные способы являются необходимым криминообразующим элементом объективной стороны состава преступления, но реализуются только в рамках основных способов совершения преступления.

При этом конкуренции между основными и специальными способами преступления не происходит, поскольку они имеют совершенно разную природу. Если обман и злоупотребление доверием являются способами хищения чужого имущества, то ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство представляют из себя способы применения орудий рассматриваемого преступления в рамках обмана и злоупотребления доверием.

Уголовный закон не содержит разъяснения существа данных способов. Частично описание данных способов совершения преступления можно обнаружить в Методических рекомендациях Генеральной прокуратуры РФ. В науке уголовного права определение сущности данных способов, как правило, дискуссий не вызывает.

Так, под вводом компьютерной информации следует понимать размещение сведений о средствах хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных

сетей для последующей обработки и (или) хранения данных сведений[30]. Определение данного понятия в Методических рекомендациях (далее - Рекомендации) Генеральной прокуратуры РФ не обнаруживается, поскольку данный способ не предусматривается в ст. ст. 272 - 274 УК РФ, для разъяснения которых были разработаны данные Рекомендации.

Что касается удаления компьютерной информации, то следует отметить, что Рекомендации также не знают данного термина, зато оперируют понятием «уничтожение информации», включенным в способ ст. 272 УК РФ.

А.А. Южин при этом отмечает, что термин «удаление», примененный в диспозиции ст. 159.6 УК РФ, не отражает существа предусмотренного законодателем способа, поскольку «любую удаленную информацию можно восстановить»[31].

Действительно, согласно толкованию С.И. Ожегова, удалить – «отдалить на какое-либо расстояние, заставить уйти куда-нибудь»[32]. То есть данное понятие не предусматривает возможность восстановления объекта. При этом исследователи понимают термин «удалить» в контексте исследуемой нормы как совершение действий, в результате которых становится невозможным восстановить содержание компьютерной информации[33]. Вместе с тем очевидно, что мошенничество в сфере компьютерной информации может быть совершено как путем удаления информации с возможностью ее восстановления, так и путем полного ее уничтожения, без возможности восстановления. В этом плане существующее понимание термина «уничтожение», более приемлемо. Под уничтожением принято понимать приведение информации или ее части в непригодное для

---

[30] Гладких, В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. N 22. С. 28.

[31] Южин, А.А. Дискуссионные вопросы мошенничества в сфере компьютерной информации // Право и кибербезопасность. 2014. N 2. С. 17.

[32] Ожегов, С.И. Словарь русского языка: ок. 53 000 слов / Под ред. Л.И. Скворцова. 24-е изд., испр. М. : Оникс, 2015. 940.

[33] Гладких, В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. N 22. С.27.

использования состояние независимо от возможности ее восстановления[34]. Представляется, что для устранения противоречия в понимании сущности способов совершения мошенничества в диспозиции ст. 159 УК РФ слово «удаления» следует заменить на слово «уничтожения».

Под блокированием информации следует понимать такое воздействие на компьютерную информацию или технику, последствием которого является невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме. При этом блокирование информации, хотя ограничивает или закрывает доступ к компьютерному оборудованию и находящимся на нем ресурсам, не предполагает удаление компьютерной информации.

Под модификацией компьютерной информации принято понимать внесение изменений в компьютерную информацию (или ее параметры).

Наибольшее количество нареканий со стороны исследователей вызывает такой способ совершения преступления, как иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей[35], не имеющее легитимного разъяснения и носящее условный характер. При этом его понимание, в сущности, не вызывает затруднений.

П.С. Яни под подобным вмешательством понимает всякое вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, если его следствием стало незаконное завладение имуществом либо приобретение права на имущество[36]. В.И. Гладких под таким вмешательством понимает осуществление неправомерных действий, нарушающих установленный процесс обработки,

---

[34] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817/

[35] Яни, П.С. Специальные виды мошенничества // Законность. 2015. N 8. С. 37.

[36] Там же. С.38.

хранения, использования, передачи и иного обращения с компьютерной информацией[37]. В сущности, представляется, что характер такого вмешательства может быть абсолютно любой, в том числе не связанный с причинением вреда компьютерной информации и средствам хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей.

Интересно в этой связи решение апелляционной инстанции на апелляционное представление государственного обвинителя, просящего отменить приговор суда первой инстанции, переквалифицировавшего деяние г-на Д. с ч. 3 ст. 159 УК РФ на ст. 159.6 УК РФ. Государственный обвинитель, мотивируя свою позицию, отметил, что виновный незаконно добился перевыпуска сим-карт потерпевших, используя которые путем введения достоверных логина и пароля осуществлял перечисление денежных средств потерпевших через систему «Онлайн», что делает квалификацию по ст. 159.6 УК РФ несостоятельной. На это суд апелляционной инстанции отметил, что, несмотря на то что виновный использовал подлинные логин и пароль при совершении преступления, оно не может рассматриваться как простое мошенничество[38]. Как мы видим, суд оценил действия виновного именно как вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей, при этом с компьютерной информацией никаких манипуляций не производилось.

Подводя итог изложенному, отметим, что оценка способов совершения мошенничества в сфере компьютерной информации должна строиться с учетом двухуровневого подхода. Первый уровень образуют способы совершения мошенничества как такового - обман и злоупотребление доверием, которые следует рассматривать в качестве основных способов

---

[37] Гладких, В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. N 22. С. 28.

[38] Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076. [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=MARB;n=520697

совершения преступления. В рамках данных способов совершения преступления реализуются ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство, которые следует воспринимать в рамках второго уровня как специальные способы совершения преступления. Специальные способы являются необходимым криминообразующим элементом объективной стороны состава преступления, но реализуются только в рамках основных способов совершения преступления. В составе преступления, предусмотренного ст. 159.6 УК РФ, они характеризуют способ воздействия на средства преступления.

2.3 Проблемы квалификации преступлений в сфере компьютерной информации со смежными составами и их предупреждение

С момента введения в действие нормы о компьютерном мошенничестве в научной литературе не затихают споры относительно необходимости ее существования в уголовном законе вообще, учеными также доказывается неудачность самой формулировки мошенничества в сфере компьютерных технологий на предмет адресата обмана в частности[39], однако, скорее всего, правоприменителя в большей мере интересуют вопросы прикладного свойства. Проведенный анализ судебной практики свидетельствует об определенных сложностях при отграничении состава преступления, предусмотренного статьей 159.6 УК РФ от смежных, а также проблемы квалификации по совокупности.

В объективной действительности хищения с использованием компьютерных технологий совершаются различными способами, однако законодатель фактически вынуждает правоприменителя квалифицировать

[39] Петров, С.В. Организованная преступность в современной России — состояние, тенденции, проблемы противодействия // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 3 (35). С. 77.

такие преступления по статье 159.6 УК РФ. Например, когда с использованием компьютерных технологий совершается тайное хищение имущества, на практике имеют место квалификация и по статье 158 УК РФ и по статье 159.6 УК РФ при сходных обстоятельствах. Подобную противоречивую квалификацию можно встретить в случаях, когда правоохранительные органы исходят из того, что не все устройства именуются компьютерами.

Так, Г., заключив договор на обслуживание с компанией сотовой связи, обнаружил, что номер его сим-карты подключен к банковской карте другого лица. Г. произвел перевод денежных средств с банковской карты потерпевшего на счет своего друга З. З. вместе с Г. распорядились данными средствами по своему усмотрению. Действиям Г. и З. судом была дана оценка как кража по пункту «а» части 2 статьи 158 УК РФ. Органы предварительного следствия и суд посчитали, что средства связи, а именно мобильный телефон, не относятся к средствам хранения, обработки и передачи компьютерной информации. По мнению правоохранительных органов и суда, сеть оператора сотовой связи не является информационно-телекоммуникационной сетью[40].

Аналогичный подход имеет место в другом уголовном деле. С. случайно выяснил, что номер его сим-карты привязан к банковскому счету другого лица. Он решил перевести денежные средства с чужого счета на свой посредством смс-сообщений со своего мобильного телефона. Приговором Свердловского районного суда г. Белгорода от 13 июня 2013 года С. признан виновным в совершении преступления, предусмотренного частью 1 статьи 158 УК РФ. В ходе следствия ему вменялось еще обвинение по части 2 статьи 272 УК РФ. Исключая из обвинения часть 2 статьи 272 УК РФ, суд посчитал, что в обвинительном заключении не отражены признаки неправомерного доступа к компьютерной информации, а также

[40] Приговор Ленинского районного суда г. Кирова. Дело № 1-674/2013. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

неподтверждения наступления последствий в виде блокирования, модификации и копирования компьютерной информации, таким образом, предъявленное в этой части обвинение С. не содержит признаков состава преступления, предусмотренного частью 2 статьи 272 УК РФ, так как действия подсудимого являются исключительно способом совершения тайного хищения денежных средств[41].

Иную квалификацию подобного деяния можно встретить в приговоре Грачевского районного суда (Ставропольский край) от 13 июня 2013 года, где Н. признана виновной в совершении преступления, предусмотренного частью 1 статьи 159.6 УК РФ. Н., также воспользовалась возможностью перевести на свой счет денежные средства с чужого счета, «привязанного» к номеру мобильного телефона[42].

Противоречивый подход имеет место и в научной литературе. Так, С. Смолин, указывая на существенное в последнее время распространение технических устройств, имеющих процессоры и собственное программное обеспечение с выходом в интернет, фактически отождествляет такие разноплановые аппараты, как сотовые телефоны, смартфоны, платежные терминалы и контрольно-кассовые машины[43], но если смартфон и обладает функциональностью карманного персонального компьютера, то контрольно-кассовая машина компьютером не является. Ее назначение состоит только в регистрации приобретения товара и фиксации кассового чека.

Данное обстоятельство, очевидно, должно привести к необходимости определения термина «компьютер». Так, О.Я. Баев, В.А. Мещеряков предлагают основывать данное понятие на информации из специальной литературы по кибернетике, где теоретическим обязательным признаком признания любого устройства компьютерным является определение

---

[41] Приговор Свердловского районного суда г. Белгорода. Дело № 1-64/2013. [Электронный ресурс]. – Режим доступа: https://sverdlovskyblg.sudrf.ru

[42] Приговор Грачевского районного суда (Ставропольский край). Дело № 2/35/2013. [Электронный ресурс]. – Режим доступа: http://sudact.ru/regular/docsnippet

[43] Смолин, С.А. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений. – М.: Юрайт, 2016. С.62.

конечности или бесконечности автоматной модели, лежащей в его основе. В результате авторы приходят к выводу о необходимости проведения каждый раз экспертизы на предмет отнесения того или иного аппарата к компьютеру[44].

Таким образом, не имеет принципиального значения как именовать то или иное техническое устройство, важнее определить его возможности, то есть имеет ли возможность тот или иной аппарат передавать, хранить, модифицировать компьютерные данные, поэтому в приведенных выше примерах правильнее выглядит квалификация по статье 159.6 УК РФ.

Отдельного внимания заслуживает вопрос о конкуренции и (или) совокупности статьи 159.6 УК РФ с другими составами. Проблем разграничения статьи 159 УК РФ и статьи 159.6 УК РФ не возникает, так как доктриной уголовного права давно выработан подход, согласно которому при конкуренции общей и специальной нормы, квалификация должна осуществляться по специальной, то есть по статье 159.6 УК РФ, а в соответствии с частью 3 статьи 17 УК РФ совокупность преступлений в этом случае отсутствует.

Отсутствует совокупность преступлений и в случаях, когда статья Особенной части УК РФ предусматривает другое преступление в качестве обстоятельства, влекущего более строгое наказание (ч. 1 ст. 17 УК РФ). Сравнивая санкции статьи 159.6 и статьи 272 УК РФ, можно увидеть, что данное правило может применяться в случаях совершения компьютерного мошенничества организованной группой, за которое наказание предусмотрено вплоть до 10 лет лишения свободы, тогда как наказание за неправомерный до-

ступ к компьютерной информации, совершенный организованной группой, наказывается до 5 лет лишения свободы, а также при совершении компьютерного мошенничества, причинившего крупный ущерб, либо лицом

[44] Баев, О.Я., Мещеряков, В.А. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. № 1 (68). С. 17.

с использованием своего служебного положения. В остальных случаях, очевидно, требуется дополнительная квалификация по статье 272 УК РФ.

В литературе по этому вопросу имеют место достаточно категоричные формулировки. Так, З.И. Хисамова пишет, что статья 159.6 УК РФ является специальной по отношению к статьям 272, 273 УК РФ. Суть ее рассуждений заключается в том, что неправомерный доступ к компьютерной информации из корыстной заинтересованности является действием, направленным на хищение, следовательно, компьютерная информация выступает средством доступа к чужому имуществу, что входит в объективную сторону статьи 159.6 УК РФ. В силу требований части 3 статьи 17 УК РФ дополнительной квалификации по статьям 272, 273 УК РФ не требуется[45].

Следует учитывать то обстоятельство, что способы совершения компьютерного мошенничества лишь отчасти перекликаются с указанными в диспозиции статьи 272 УК РФ способами. Законодатель использует термин «иное вмешательство» в статье 159.6 УК РФ, что позволяет утверждать, что способов совершения компьютерного мошенничества больше. Кроме того, при совершении мошенничества в сфере компьютерной информации доступ к этой информации может носить как законный, так и незаконный характер, тогда как в статье 272 УК РФ речь идет о неправомерном доступе к охраняемой законом компьютерной информации.

Скорее всего, на данном обстоятельстве и следует строить ответ на вопрос о совокупности или отсутствии таковой составов преступлений, предусмотренных статьей 159.6 УК РФ и статьей 272 УК РФ, так как санкция статьи 159.6 УК РФ не позволяет дать однозначный ответ в соответствии с правилом, изложенным в части 1 статьи 17 УК РФ.

Учитывая, что состав преступления, предусмотренный статьей 159.6 УК РФ, относится к числу сложных преступлений, которые могут совершаться посредством других преступлений-способов, необходимо

[45] Хисамова, З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1 (55). С. 118.

выработать общий подход к правилам квалификации в подобных случаях. Можно сказать, что, если способ совершения преступления является самостоятельным преступлением, его вменение по совокупности с основным преступлением не требуется. Такой вывод можно сделать на основе правила о конкуренции общего и части, однако данное правило, хотя и взятое нами за основу, не во всех случаях применимо. В.С. Минская, придерживаясь аналогичной позиции, добавляла, что преступление-способ не может вменяться только в том случае, если по тяжести он ниже основного состава преступления. В случае если тяжесть преступления-способа совпадает с основным преступлением, а тем более если выше, то требуется дополнительная квалификация[46]. Кроме того, еще одним условием отсутствия совокупности преступлений должно быть единство объекта. Относительно квалификации статьи 272 УК РФ с иными составами преступлений, где неправомерный доступ является преступлением-способом, В.С. Минская указывала на необходимость определения вида совокупности: при реальной совокупности должна быть квалификация и по статье 272 и по основному составу, при идеальной совокупности оценка преступных действий дается только по основному составу, то есть в нашем случае только по статье 159.6 УК РФ.

Приведенные правила квалификации рассмотрим на конкретном примере. Так, Б.Н., Б.С., С.В. путем установки в Белгороде на банкоматы ОАО «Сбербанк России» устройства, предназначенного для негласного получения информации, намеревались совершить хищение денежных средств со счетов клиентов банков. Они предполагали считать электронную информацию с карты памяти неизвестного устройства, крепившегося ими на банкоматы, и далее передать ее изготовителю поддельных карт, но в силу того, что они были задержаны сотрудниками полиции, довести свой преступный умысел до конца им не удалось. Все подсудимые были признаны

[46] Минская В.С. Современное законодательное регулирование уголовной ответственности за мошенничество и вопросы квалификации // Законы России: опыт, анализ, практика. 2013. N 10. С. 36.

виновными в совершении преступлений, предусмотренных частью 2 статьи 35, частью 3 статьи 183; частью 3 статьи 30, частью 2 статьи 159.6 УК РФ[47].

Данный пример заставляет усомниться в правильности квалификации действий виновных. Так называемый скиминг — противоправные действия по установке накладки на банкомат для считывания пин-кода, которая в приведенном примере именуется как «устройство, предназначенное для негласного получения информации», полностью подпадает под признаки статьи 187 УК РФ, так как такое техническое устройство предназначено для неправомерного осуществления приема, выдачи и перевода денежных средств, однако в вину осужденным не вменялось изготовление (либо приобретение) в целях использования технических устройств, предназначенных для неправомерного осуществления приема, выдачи, перевода денежных средств. Собирание сведений, составляющих банковскую тайну (ст. 183 УК РФ), является по отношению к статье 187 УК РФ преступлением-способом. Родовой объект преступлений совпадает. Преступление, предусмотренное частью 1 статьи 183 УК РФ, относится к категории небольшой тяжести, а преступление, предусмотренное частью 1 статьи 183 УК РФ, — к категории средней тяжести.

Учитывая условия, предложенные ранее, квалификация должна осуществляться только по части 1 статьи 183 УК РФ. Что касается совокупности (или отсутствия таковой) в приведенном примере с частью 2 статьи 159.6 УК РФ, то, следуя все тем же условиям оценки признания в действиях виновных совокупности преступлений, признание судом покушения на мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору, на наш взгляд, является справедливым.

Таким образом, можно считать, что правильней квалификация действия виновных должна выглядеть следующим образом: часть 1 статьи 187; часть 3

---

[47] Приговор Свердловского районного суда г. Белгорода. Дело № 1-64/2013. [Электронный ресурс]. – Режим доступа: https://sverdlovskyblg.sudrf.ru

статьи 30, часть 2 статьи 159.6 УК РФ. К сожалению, приходится констатировать тот факт, что игнорирование практикой нормы о неправомерном обороте средств платежей является скорее правилом, чем исключением.

В практике имеют место ситуации, когда правоприменитель не обнаруживает признаков преступления, предусмотренного статьей 159.6 УК РФ, и инкриминирует лишь статью 187 УК РФ либо наоборот. Так, Ф., являясь руководителем ООО «С…», в целях обналичивания денежных средств изготовил несколько платежных поручений. Он создал на имя М. юридические лица, после чего М. открыл счета на созданные компании в Пробизнесбанке. Получив возможность осуществлять безналичные расчеты от имени данных юридических лиц, Ф. создавал платежные поручения для перевода денежных средств на другие подконтрольные ему счета[48]. Суд указал, что Ф. сбывал платежные поручения. Но скорее всего, платежные поручения Ф. использовал для дальнейшего обналичивания денежных средств, что говорит о необходимости квалификации его действий и по статье 159.6 УК РФ.

В другом уголовном деле действиям К. суд также не дал юридическую оценку по наличию в его действиях признаков состава преступления, предусмотренного статьей 159.6 УК РФ. К. как учредитель и директор ООО, пользуясь возможностью электронного документооборота, передавал распоряжения обслуживающему счет потерпевшего Ф. банку на перевод денежных сумм потерпевшего на счет получателя. В этих целях он сформировал распоряжение о переводе денежных средств. Данные действия он совершал неоднократно. Суд посчитал, что К. совершил неправомерный оборот средств платежей и признал его виновным по части 1 статьи 187 УК РФ[49].

---

[48] Приговор Заводского районного суда г. Орла. Дело №1-114/2013. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

[49] Приговор Индустриального районного суда г. Ижевска. Дело № 1-311/2016. [Электронный ресурс]. – Режим доступа: http://судебные-решения.рф/bsr/case

Противоположную позицию по уголовному делу при сходных обстоятельствах можно обнаружить в приговоре Черемушкинского районного суда г. Москвы, однако в жалобе адвоката имеет место лишь несогласие с квалификацией по статье 159.6 УК РФ. По его мнению, действия подзащитного должны быть квалифицированы по статье 159 УК РФ[50]. Московский городской суд, не соглашаясь с доводами адвоката, оставил квалификацию без изменения. Обращает на себя внимание то обстоятельство, что ни следствие, ни суд обеих инстанций вопрос о наличии в действиях виновного признаков преступления, предусмотренного статьей 187 УК РФ, даже не ставился, хотя данный состав преступления относится к более высокой категории преступления.

Совершенно верную, на наш взгляд, квалификацию дал Верховный Суд Чувашской Республики, признав М. виновным по статье 159.6 УК РФ и оправдав по части 1 статьи 187 УК РФ только лишь по факту того, что на момент совершения деяний, действовала предыдущая редакция статьи 187 УК РФ, не признававшая распоряжения о переводе денежных средств платежными документами. Важно то, что суд не поставил под сомнение правильность квалификации преступлений по статье 159.6 и статье 187 УК РФ по совокупности[51].

При квалификации деяний правоприменитель должен исходить из того, на каких основаниях, то есть законных или незаконных, виновное в хищении лицо получило доступ к компьютерной информации. В случае законного доступа к такой информации дополнительной квалификации по статьям 187, 272, 273 УК РФ не требуется.

Итак, действующая редакция статьи 159.6 УК РФ нуждается в разъяснениях Пленума Верховного Суда РФ. Полагаем, с учетом сложившейся правоприменительной практики и доктринального толкования

---

[50] Приговор Черемушкинского районного суда г. Москвы от 5 марта 2015 г. [Электронный ресурс]. – Режим доступа: http://судебныере-шения.рф/bsr/case

[51] Апелляционное определение Верховного Суда Чувашской Республики. Дело № 22-1380/2016. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

форм хищения, судам следует дать разъяснения, что в случае, если 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 осуществляется с участием лица, воспринимающего искаженную информацию как истинную, например, «фишинг», смс-мошенничество, платный просмотр видеорекламы и т. п., содеянное следует квалифицировать как мошенничество в сфере компьютерной информации.

В случае осуществления хищения тем же способом, но без непосредственного участия человека, например, посредством использования автоматизированных систем, содеянное следует квалифицировать как кражу.

При решении вопроса о совокупности преступлений, например, со статьями 183, 187, 272, 273 УК РФ, необходимо учитывать ряд условий:

— определять основания доступа к компьютерной информации;

— если доступ осуществлялся незаконно, правоприменитель должен дать юридическую оценку таких действий, основываясь на таких условиях квалификации как единство родового объекта и категория преступления. Учитывая, что часть 1 статьи 159.6 УК РФ относится с категории преступлений небольшой тяжести, данное обстоятельство свидетельствует о необходимости дополнительной квалификации по соответствующей статье УК РФ, являющейся по отношению к статье 159.6 УК РФ преступлением-способом независимо от совпадения либо несовпадения родового объекта.

Что касается аспекта совершенствования законодательства в представленной сфере, то стоит обозначить, что в уголовно-правовой науке сформировалось два основных направления по решению проблем законодательства в части квалификации преступлений в сфере компьютерной информации.

Согласно первому направлению, в ряд составов («Нарушение авторских и смежных прав», «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», «Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники» и так далее) необходимо ввести такой способ совершения преступления, как «с применением компьютерных средств» (выдвигаются и такие трактовки, как «...с применением компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, системы или сети связи, иных высокотехнологичных и научно-технических средств», «с применением информационных технологий» и так далее)[52]. Причём представленное направление частично уже апробировано законодателем. Так, в Уголовный кодекс Российской Федерации был внесен новый состав мошенничества – «Мошенничество в сфере компьютерной информации». Данный состав закрепил за собой ответственность за мошенничество в данной сфере, то есть хищение чужого имущества или приобретения права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей. Казалось бы, что типичной формой мошенничества является его совершение с использованием сети Интернет, однако регулирование сферы, касающейся Интернета как компьютерной сети, не носило правового характера и относилось лишь к области технических стандартов. Это при том, что сотрудниками правоохранительных органов был обозначен ряд проблем, которые возникали при квалификации мошенничества в сфере высоких технологий, в

[52] Нагорный, А.А. Проблемы квалификации преступлений в сфере компьютерной информации [Электронный ресурс]. – Режим доступа: http://oaji.net/articles/2014/245–1393744181.pdf

котором не задействованы ни ЭВМ, ни система ЭВМ и их сети. То есть, это весьма точное и отвечающее современным реалиям правоприменительного толка нововведение, так как до принятия поправки мошенничество путём неправомерного доступа к компьютерной информации требовало квалификации по совокупности преступлений «Мошенничество» и «Неправомерный доступ к компьютерной информации». То есть, одним действием лицо совершало два преступления. Теперь же достаточно квалификации по статье «Мошенничество в сфере компьютерной информации», что ведёт к логичному упрощению процесса уголовного судопроизводства[53].

Согласно второму направлению, необходимо введение отдельного раздела в Уголовный кодекс Российской Федерации, который бы был полностью сконцентрирован на компьютерных преступлениях. Однако, во-первых, в данном случае нарушается системность уголовного законодательства. А, во-вторых, вопрос об определенности перечня компьютерных преступлений по-прежнему остаётся нерешённым.

Поскольку утвердительно положительная динамика сферы компьютерной информации оказывает весьма заметное влияние на новые виды и формы преступлений, что, в свою очередь, проявляет прямое воздействие на понятийный аппарат и сложность квалификации преступных деяний, то и реакция законодателя должна быть оперативной и соответствовать правоприменительным реалиям. В российской уголовно-правовой науке выработалось два основных курса, направленных на решение проблем законодательства в части квалификации преступлений в сфере компьютерной информации. Причём некоторые выведенные из этих курсов нововведения активно применяются на практике. Однако специфика сферы компьютерной информации диктует необходимость постоянного комплексного совершенствования уголовного законодательства.

---

[53] Лысак, Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2013. – №90. С.45.

Заключение

Поскольку компьютерная информация не является материальным предметом, иногда бывает достаточно сложно не только определить состав преступления при ее хищении, но и непосредственно это хищение зафиксировать. Невозможности назначит наказание за подобные преступления способствует и компьютерная неграмотность населения. Из-за этого огласке, и вынесению дела в суд предаются только особо громкие случаи, повлекшие за собой сбой в работе крупных организаций.

В России глава УК, соответствующая компьютерным преступлениям, была разработана и принята только в 1997 году. По сравнению с западными странами, ведущими дела в этой сфере уже с 70-х годов, у нас еще не накоплен достаточный опыт, позволяющий компетентно рассматривать данные правонарушения. Более того, в российском законодательстве пока еще нет документов, которые могли бы регламентировать компьютерные доказательства.

Что касается аспекта совершенствования законодательства в представленной сфере, то стоит обозначить, что в уголовно-правовой науке сформировалось два основных направления по решению проблем законодательства в части квалификации преступлений в сфере компьютерной информации.

Согласно первому направлению, в ряд составов («Нарушение авторских и смежных прав», «Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну», «Незаконные экспорт из Российской Федерации или передача сырья, материалов, оборудования, технологий, научно-технической информации, незаконное выполнение работ (оказание услуг), которые могут быть использованы при создании оружия массового поражения, вооружения и военной техники» и так далее) необходимо ввести такой способ совершения

преступления, как «с применением компьютерных средств» (выдвигаются и такие трактовки, как «...с применением компьютерной информации, ЭВМ, системы ЭВМ, сети ЭВМ, системы или сети связи, иных высокотехнологичных и научно-технических средств», «с применением информационных технологий» и так далее)[54]. Причём представленное направление частично уже апробировано законодателем. Так, в Уголовный кодекс Российской Федерации был внесен новый состав мошенничества – «Мошенничество в сфере компьютерной информации».

Данный состав закрепил за собой ответственность за мошенничество в данной сфере, то есть хищение чужого имущества или приобретения права на чужое имущество путём ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-коммуникационных сетей. Казалось бы, что типичной формой мошенничества является его совершение с использованием сети Интернет, однако регулирование сферы, касающейся Интернета как компьютерной сети, не носило правового характера и относилось лишь к области технических стандартов. Это при том, что сотрудниками правоохранительных органов был обозначен ряд проблем, которые возникали при квалификации мошенничества в сфере высоких технологий, в котором не задействованы ни ЭВМ, ни система ЭВМ и их сети. То есть, это весьма точное и отвечающее современным реалиям правоприменительного толка нововведение, так как до принятия поправки мошенничество путём неправомерного доступа к компьютерной информации требовало квалификации по совокупности преступлений «Мошенничество» и «Неправомерный доступ к компьютерной информации». То есть, одним действием лицо совершало два преступления. Теперь же достаточно квалификации по статье «Мошенничество в сфере компьютерной

[54] Нагорный, А.А. Проблемы квалификации преступлений в сфере компьютерной информации [Электронный ресурс]. – Режим доступа: http://oaji.net/articles/2014/245–1393744181.pdf

информации», что ведёт к логичному упрощению процесса уголовного судопроизводства[55].

Согласно второму направлению, необходимо введение отдельного раздела в Уголовный кодекс Российской Федерации, который бы был полностью сконцентрирован на компьютерных преступлениях. Однако, во-первых, в данном случае нарушается системность уголовного законодательства. А, во-вторых, вопрос об определенности перечня компьютерных преступлений по-прежнему остаётся нерешённым.

Поскольку утвердительно положительная динамика сферы компьютерной информации оказывает весьма заметное влияние на новые виды и формы преступлений, что, в свою очередь, проявляет прямое воздействие на понятийный аппарат и сложность квалификации преступных деяний, то и реакция законодателя должна быть оперативной и соответствовать правоприменительным реалиям. В российской уголовно-правовой науке выработалось два основных курса, направленных на решение проблем законодательства в части квалификации преступлений в сфере компьютерной информации. Причём некоторые выведенные из этих курсов нововведения активно применяются на практике. Однако специфика сферы компьютерной информации диктует необходимость постоянного комплексного совершенствования уголовного законодательства.

[55] Лысак, Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2013. – №90. С.45.

Список используемых источников

1. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (ред. от 21.07.2014) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_28399/

2. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 25.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_10699/

3. Гражданский кодекс Российской Федерации часть 4 18 декабря 2006 года N 230-ФЗ (ред. от 01.07.2017) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_64629/

4. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 23.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/

5. Закон РФ от 27.12.1991 N 2124-1 «О средствах массовой информации» (ред. от 18.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_1511/

6. Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне» (ред. от 26.07.2017) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_2481/

7. Федеральный закон «О связи» от 07.07.2003 N 126-ФЗ (ред. от 18.04.2018) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_43224/

8. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации (утв. Генпрокуратурой России) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_161817/

9. Баев, О.Я., Мещеряков, В.А. Понятие «компьютерная информация» в российском уголовном праве // Вестник Восточно-Сибирского института Министерства внутренних дел России. 2014. № 1 (68). С. 16—20.

10. Бегишев, И.Р. Ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей // Вестник УРФО. Безопасность в информационной среде. 2012. N 1. С. 15 - 18.

11. Быков, В.М., Черкасов, В.Н. Понятие компьютерной информации как объекта преступлений // Законность. 2013. N 12. С. 37 - 40.

12. Быков, В.М., Черкасов, В.Н. Новый закон о преступлениях в сфере компьютерной информации: ст. 272 УК РФ // Российский судья. 2012. N 5. С. 14 – 19.

13. Гладких, В.И. Компьютерное мошенничество: а были ли основания его криминализации? // Российский следователь. 2014. N 22. С. 27 - 28.

14. Елин, В.М. Неправомерный доступ к компьютерной информации // Бизнес-информатика. 2013. N 2. С. 70 - 76.

15. Ефремова, М.А. К вопросу о понятии компьютерной информации // Российская юстиция. 2012. N 7.

16. Ефремова М.А. Мошенничество с использованием электронной информации // Информационное право. 2013. N 4. С. 19 - 21.

17. Звонов, А.В. Система мер уголовно-правового воздействия: сущность и содержание // Человек: преступление и наказание. 2015. N 3. С. 95 – 99.

18. Камышов Д.А. Понятие и признаки мошенничества в Российском уголовном законодательстве // Проблемы в Российском законодательстве. 2012. N 2. С. 147 – 151.

19. Количество пользователей интернета в России // Интернет в России и в мире [Электронный ресурс]. – Режим доступа: http://www.bizhit.ru/index/users_count/0–151

20. Лысак, Е.А. Проблемы квалификации преступлений в сфере компьютерной информации // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2013. – №90.

21. Минская В.С. Современное законодательное регулирование уголовной ответственности за мошенничество и вопросы квалификации // Законы России: опыт, анализ, практика. 2013. N 10. С. 35 - 38.

22. Нагорный, А.А. Проблемы квалификации преступлений в сфере компьютерной информации [Электронный ресурс]. – Режим доступа: http://oaji.net/articles/2014/245–1393744181.pdf

23. Кондратов, М.А. К постановке вопроса об уголовной ответственности юридических лиц в уголовном праве России (исторический аспект) / М.А. Кондратов, С.С. Медведев // Научный журнал КубГАУ – Scientific Journal of KubSAU. – 2015. – №106.

24. Ожегов, С.И. Словарь русского языка: ок. 53 000 слов / Под ред. Л.И. Скворцова. 24-е изд., испр. М. : Оникс, 2015. 1080 с.

25. Петров, С.В. Организованная преступность в современной России — состояние, тенденции, проблемы противодействия // Юридическая наука и практика: Вестник Нижегородской академии МВД России. 2016. № 3 (35). С. 77—80.

26. Пионтковский, А.А. Курс советского уголовного права: В шести томах / Редакционная коллегия: А.А. Пионтковский, П.С. Ромашкин, В.М. Чхиквадзе. М.: Наука, 1970. Часть общая. Том II. Преступление.

27. Смолин, С.А. Уголовно-правовая борьба с высокотехнологичными способами и средствами совершения преступлений. – М.: Юрайт, 2016. – 201 с.

28. Хилюта, В.В. Уголовная ответственность за хищения с использованием компьютерной техники // Журнал российского права. 2014. N 3. С. 111 – 118.

29. Хисамова, З.И. Об особенностях квалификации преступлений, совершаемых в сфере использования информационно-коммуникационных технологий // Общество и право. 2016. № 1 (55). С. 118—201.

30. Чекунов, И.Г. Компьютерная преступность: законодательная и правоприменительная проблемы компьютерного мошенничества // Российский следователь. 2015. N 17. С. 29 - 33.

31. Черкасов, В.Н. Дискретность интеллектуальной собственности, или С чего начинается копия? // Защита информации. Инсайт. 2011. N 2(38).

32. Чуриков, Н.А. Преступления в сфере компьютерной информации: проблемы квалификации и совершенствования уголовного законодательства в данной сфере / Н.А. Чуриков, С.С. Медведев // Образование и наука в современных реалиях : материалы Междунар. науч.–практ. конф. (Чебоксары, 4 июня 2017 г.). В 2 т. Т. 2 / редкол.: О.Н. Широков [и др.] – Чебоксары: ЦНС «Интерактив плюс», 2017. – С. 312-317.

33. Южин, А.А. Дискуссионные вопросы мошенничества в сфере компьютерной информации // Право и кибербезопасность. 2014. N 2.

34. Яни, П.С. Специальные виды мошенничества // Законность. 2015. N 8. С. 35 - 40.

35. Апелляционное определение Верховного Суда Чувашской Республики. Дело № 22-1380/2016. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

36. Апелляционное определение Московского городского суда от 6 мая 2013 г. N 10-2076. [Электронный ресурс]. – Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=MARB;n=520697

37. Приговор Ленинского районного суда г. Кирова. Дело № 1-674/2013. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

38. Приговор Свердловского районного суда г. Белгорода. Дело № 1-64/2013. [Электронный ресурс]. – Режим доступа: https://sverdlovskyblg.sudrf.ru

39. Приговор Грачевского районного суда (Ставропольский край). Дело № 2/35/2013. [Электронный ресурс]. – Режим доступа: http://sudact.ru/regular/docsnippet

40. Приговор Заводского районного суда г. Орла. Дело №1-114/2013. [Электронный ресурс]. – Режим доступа: http://судебныерешения.рф/bsr/case

41. Приговор Индустриального районного суда г. Ижевска. Дело № 1-311/2016. [Электронный ресурс]. – Режим доступа: http://судебные-решения.рф/bsr/case

42. Приговор Черемушкинского районного суда г. Москвы от 5 марта 2015 г. [Электронный ресурс]. – Режим доступа: http://судебныере-шения.рф/bsr/case

43. Уголовное дело N 1-90/2013. Архив Первомайского районного суда г. Пензы за 2013 г. [Электронный ресурс]. – Режим доступа: http://pervomaisky.pnz.sudrf.ru/modules.php?name=norm_akt&id=124