Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра уголовного права

УТВЕРЖДАЮ
Заведующий кафедрой

_____ А. Н. Тарбагаев
подпись инициалы, фамилия

«____» _____ 2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

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

40.04.01 – Юриспруденция
код и наименование направления

40.04.01.01 – Правосудие по уголовным делам
код и наименование магистерской программы

Научный руководитель _____ доцент, к.ю.н. В.В. Питецкий
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник _____ А. О. Надводнюк
подпись, дата инициалы, фамилия

Рецензент _____ прокурор Манского района, старший советник юстиции С.Н. Коряков
подпись, дата должность, звание инициалы, фамилия

Красноярск, 2020

АННОТАЦИЯ

В магистерской диссертации рассматриваются вопросы квалификации преступления, предусмотренного ст. 272 УК РФ (Неправомерный доступ к компьютерной информации). В работе исследованы объективные и субъективные признаки преступления, проанализированы квалифицирующие признаки. В настоящий момент, правильное применение нормы вызывает затруднения в связи с наличием технических терминов, неопределенностью приведенных понятий, а также субъективной стороны преступления, наличием конкурирующих смежных составов и иных преступлений.

Методология исследования. Методологической основой исследования являются положения диалектического метода. Также были использованы такие методы, как сравнение, метод анализа и синтеза, описания, сравнительного правоведения.

Ключевые слова: компьютерная информация, неправомерный доступ, уничтожение компьютерной информации, копирование компьютерной информации, блокирование компьютерной информации, модификация компьютерной информации.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность исследования. На данный момент развитие информационных технологий растет. Использование информационных технологий привело к увеличению роста преступности.

Компьютерные преступления являются преступлениями информационного характера, а также носят трансграничный, международный характер. Следовательно, необходимость защиты отношений в этой сфере очевидна.

На законодательном уровне существуют множество актов, регулирующих такие отношения, в том числе и устанавливающих ответственность за совершение таких преступлений.

Так как эти преступления носят международный характер, то в первую очередь к актам, регулирующим такие отношения необходимо отнести Европейскую конвенцию по киберпреступлениям, в которой сказано, что компьютерные сети и электронная информация могут также использоваться для совершения преступлений, и, что эффективная борьба против киберпреступлений требует наличия четкого, быстрого и эффективного механизма международного сотрудничества в вопросах, связанных с преступностью.

В Российской Федерации, ответственность за преступления в компьютерной сфере закреплена в первую очередь в Уголовном Кодексе. Глава 28 УК РФ относит к ним такие преступления как: неправомерный доступ к компьютерной информации; создание, использование и распространение вредоносных компьютерных программ; нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Опасность преступлений в сфере компьютерной информации состоит прежде всего в том, что они оказывают негативное влияние на различные общественные отношения, охраняемые уголовным законом.

В связи с этим, законодатель отнес главу 28 «Преступления в сфере компьютерной информации» к разделу «Преступления против общественной безопасности и общественного порядка».

В числе этих преступлений находится и неправомерный доступ к компьютерной информации, предусмотренный ст. 272 УК РФ.

Цель данного исследования состоит в том, чтобы на основе изучения общенаучной, специальной и уголовно-правовой литературы, выявить понятие и признаки преступления, предусмотренного ст. 272 УК РФ, а также проблемные вопросы, возникающие в правоприменении.

Задачи исследования. Изучить объект и предмет неправомерного доступа к компьютерной информации. Рассмотреть объективную сторону преступления. Исследовать субъективные признаки преступления. Проанализировать квалифицирующие признаки преступления. Выявить признаки, отграничивающие преступление, предусмотренное ст. 272 УК РФ от смежных составов преступлений, а также иных преступлений.

Объектом исследования являются общественные отношения по уголовно-правовой регламентации неправомерного доступа к компьютерной информации.

Предметом исследования является норма об уголовной ответственности за неправомерный доступ к компьютерной информации.

Нормативная база исследования. Для изучения данной темы необходимо, прежде всего, обратиться к Европейской конвенции по киберпреступлениям от 21.11.2001. Также к Конституции Российской Федерации, Уголовному Кодексу Российской Федерации от 13.06.1996 № 63-ФЗ, ФЗ «Об информации, информационных технологиях и о защите информации»; Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации утв. Генпрокуратурой России от 30.05.2014, иным актам.

Теоретическая основа исследования**.** Данная проблема изучена и представлена в значительном количестве источников. Среди исследователей

данного вопроса следует, прежде всего, назвать А.Ф. Мицкевича, А.В. Суслопарова и В.Г. Степанова-Егиянца которые в своих многочисленных научных работах подробно анализируют все признаки состава рассматриваемого преступления с приведением примеров из судебной практики. Среди научных статей, посвященных исследованию рассматриваемого преступления, следует назвать работы: А. Н. Тарбагаева, В.И. Алескерова, Ю.В. Гаврилина, А. А. Фатьянова, З. Н. Индрисовой, А.И. Куприянова, М. И. Третьяка, М. А. Зубовой, А. И. Халлиулина, А.И. Абова, Р.М. Айсанова, А.Г. Волеводза, В.К. Гавло, Ю.В. Гаврилина, А.А. Гребенькова, Р.И. Дремлюги, К.Н. Евдокимовой, А.М. Ефремовой, У.В. Зининой, А.Ж. Кабановой, В.С. Карпова, В.В. Крылова, М.М. Малыковцева, Д.Г. Малышенко, А.А. Нагорного, Б.С. Никифорова, А.Ю. Решетникова, Е.А. Русскевича,

Структура работы включает введение, 3 главы, заключение и список использованных источников.

1 Анализ состава преступления, предусмотренного ст. 272 УК РФ

1.1 Объект неправомерного доступа к компьютерной информации

Объектом преступления в уголовном праве признаются те охраняемые законом общественные отношения, на которые посягает общественно-опасное и уголовно-наказуемое деяние.[1]

Важно отметить, что та охраняемая уголовным законом совокупность общественных отношений является общим объектом преступления.[2]

Родовым объектом преступления необходимо признать такую группу общественных отношений, являющихся однородными, и охраняемую уголовным законом.[3]

Родовым объектом неправомерного доступа к компьютерной информации выступают общественные отношения, обеспечивающие общественную безопасность и общественный порядок.

Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности» в ст. 1 указывает, что видом безопасности является общественная безопасность.[4]

Под безопасностью понимается состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз.[5]

Состоянием защищенности, по мнению С.В. Нестерова, следует признавать такое состояние объекта и его устойчивое развитие, характеризующееся возможностью сохранять качественную определенность, выполнять свои функции и задачи в условиях воздействия негативных

---

[1] Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 73.
[2] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 102.
[3] Уголовное право. Общая часть : учебник / под ред. И. Я. Козаченко. – Москва : Норма, 2008. С. 207.
[4] О безопасности [Электронный ресурс] : федер. закон от 28.12.2010 № 390-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru
[5] Уголовное право. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай. – 2-е изд., с изм и доп. – Москва : Инфра-М, 2008. С. 467.

факторов, в результате целенаправленной деятельности системы обеспечения безопасности.[6]

Под жизненно важными интересами понимается совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможность прогрессивного развития личности, общества и государства.[7]

К основным объектам безопасности относятся: личность – ее права и свободы, общество – его материальные и духовные ценности, государство – его конституционный строй, суверенитет и территориальную целостность.[8]

По мнению С.В. Нестерова общественная безопасность это состояние защищенности личности, общества и государства от угроз различного характера, позволяющее им сохранять качественную определенность и способствующее их устойчивому развитию.[9]

Общественная безопасность и общественный порядок – тесно связанные категории по общности цели, направленной на защиту различных интересов. Под общественным порядком понимается совокупность общественных отношений, урегулированная социальными нормами, установление, развитие и охрана которых обеспечивают поддержание общественного и личного спокойствия, уважение человеческого достоинства и общественной нравственности.[10]

Таким образом, родовым объектом неправомерного доступа к компьютерной информации являются общественные отношения, обеспечивающие общественную безопасность, а также общественный порядок.

Необходимо указать, что понимать под видовым объектом. Так обозначенные в главах Уголовного кодекса группы отношений, являющиеся

---

[6] Нестеров С. В. Понятие общественной безопасности [Электронный ресурс] / С. В. Нестеров // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2013. – № 11. – Режим доступа: http://cyberleninka.ru

[7] Уголовное право. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай. – 2-е изд., с изм и доп. – Москва : Инфра-М, 2008. С. 467.

[8] Там же.

[9] Нестеров С. В. Понятие общественной безопасности [Электронный ресурс] / С. В. Нестеров // Вестник Тамбовского университета. Серия: Гуманитарные науки. – 2013. – № 11. – Режим доступа: http://cyberleninka.ru

[10] Уголовное право. Особенная часть. : учебник / под ред. И. В. Шишко. – Москва. :Проспект, 2011. С. 399

частью родового объекта, однако объединенные в связи с их близкой взаимосвязью являются видовым объектом.[11]

Видовым объектом неправомерного доступа к компьютерной информации являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации.

Непосредственный объект – правоотношение, нарушаемое конкретным преступлением.[12]

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», под непосредственным объектом преступления, предусмотренного ст. 272 УК РФ, выступают общественные отношения, обеспечивающие правомерный доступ, создание, хранение, модификацию, использование компьютерной информации самим создателем, потребление ее иными пользователями[13]

Существуют различные точки зрения на определение понятия непосредственного объекта преступления, предусмотренного ст. 272 УК РФ.

Ряд ученых определяют непосредственный объект неправомерного доступа к компьютерной информации через понятие состояние защищенности.

Так, В.И. Алескеров, говоря об объекте данного преступления, определяет его как безопасность информационных систем, то есть такое использование информационных систем, исключающее причинение вреда обществу, личности и государству.[14]

У.В. Зинина в своей работе указывала на то, что понимать под непосредственным объектом преступления в ст. 272 УК РФ. В соответствии с позицией данного автора, такой объект преступления заключается в обеспечении

---

[11] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 103.

[12] Уголовное право. Общая часть : учебник / под ред. И. Я. Козаченко. – Москва : Норма, 2008. С. 207.

[13] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[14] Алескеров В.И. Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации: Лекция. [Электронный ресурс] / Алескеров В.И., Максименко И.А. – Домодедово: ВИПК МВД России, 2011. – Режим доступа: http://www. elibrary.ru.

безопасности осуществления и реализации полномочий субъектов – обладателей информации или субъектов, имеющих право использовать информацию в пределах, установленных нормативными актами.[15]

Согласно иному взгляду исследователей на непосредственный объект указанного преступления, для его установления необходимо выделить следующие права: право владельца на информацию и ее неприкосновенность, соответствующие права иных – третьих лиц, права физических и юридических лиц, гражданина, общества и государства по поводу владения, пользования и распоряжения компьютерной информации. Таким образом, выделяя эти права, исследователи связывали объект преступления с совокупностью вышеназванных прав.[16]

Существует другое определение непосредственного объекта данного преступления. В соответствии с ним объектом преступления, предусмотренного ст. 272 УК РФ, является безопасность использования как самой компьютерной информации, так и различных информационных систем и ресурсов.[17]

А.В. Суслопаров определяет объект данного преступления как информационное общественное отношение, которое обеспечивает информационную безопасность личности, общества и государства.[18]

В.Г. Степанов-Егиянц, критикуя подходы ученых, которые определяют объект через нарушение прав и состояние защищенности, говорит о том, что преступление изменяет общественные отношения, однако причинить вред социальному благу не способно, а также не может нарушать какое-либо состояние и чьи-то права. Преступление, прежде всего, посягает на общественные отношения. Так, общественные отношения, обеспечивающие, прежде всего, безопасность компьютерной информации, безопасность ее

[15] Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве [Электронный ресурс]: Дис. ... канд. юрид. наук.: 12.00.08 / Зинина Ульяна Викторовна. – Москва , 2007. – Режим доступа: http://www. diss.seluk.ru.

[16] Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В. Г. Степанов-Егиянц. – Москва : Статут, 2016. – Режим доступа: http://www.consultant.ru.

[17] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [Электронный ресурс] / под ред. В. М. Лебедева. – Режим доступа: http://www.consultant.ru.

[18] Суслопаров А. В. Информационные преступления : автореф. дис….канд. юридических наук : 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2008. 24 с.

средств хранения и обработки, исследователь называет непосредственным объектом неправомерного доступа к компьютерной информации. Помимо этого, в объект входят такие общественные отношения, обеспечивающие правомерный доступ к информации, то есть законное ее получение, а также использования. В заключение, необходимо добавить, что в объект входят общественные отношения, связанные с правильной работой материальных носителей информации.[19]

По нашему мнению, под непосредственным объектом преступления, предусмотренного ст. 272 УК РФ, следует понимать общественные отношения, обеспечивающие право обладателя компьютерной информации на безопасное создание компьютерной информации, ее хранение, пользование и передачу.

Дополнительный объект преступления – это общественные отношения, нуждающиеся в самостоятельной защите, которые попутно охраняются законом, но подлежат защите в связи с тем, что вред им причиняется всегда при посягательстве на основной объект преступления.[20]

Существует два вида дополнительных объектов – дополнительный обязательный и дополнительный факультативный объект. При совершении преступления вред дополнительному обязательному объекту всегда причиняется всегда. Причинение вреда дополнительному обязательному объекту должно отражаться в конкретной норме уголовного закона. Вред дополнительному факультативному объекту причиняется не всегда и его наличие зависит от особенностей конкретного преступления.[21]

Исходя из анализа статьи 272 УК РФ, можно сделать вывод о том, что дополнительный факультативный объект предусмотрен частями третьей и четвертой данной статьи.

Так, частью третьей ст. 272 УК РФ предусмотрена ответственность за неправомерный доступ к компьютерной информации, совершенный с

---

[19] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[20] Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 81.

[21] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 105.

использованием служебного положения. В данном случае, дополнительным объектом следует признать интересы службы в коммерческих и иных организациях, а также государственной службы, заключающиеся в правильном и четком функционировании аппаратов управления организаций, государственных органов и органов местного самоуправления.

При наличии других объектов, которым причиняется вред при совершении неправомерного доступа к компьютерной информации, как правило, такое деяние квалифицируется по совокупности, за исключением деяний, которые охватываются ч. 4 ст. 272 УК РФ, то есть деяния, повлекшие тяжкие последствия или создавшие угрозу их наступления.[22] Преступление, предусмотренное ч. 4 ст. 272 УК РФ будет рассмотрено нами в третьей главе.

Можно привести следующие примеры квалификации деяний по совокупности.

Так, приговором от 06.02.2019 по делу № 1-533/2018 Советского районного суда г. Томска установлено, что лицо умышлено, в целях сбыта и получения прибыли от последующей продажи копий программных продуктов путем их установки, незаконно, без заключения соответствующих соглашений с правообладателями, приобрел контрафактные экземпляры произведений – программные продукты: «Microsoft Windows 7 Профессиональная», стоимость которого составляла 127.000 рублей, после чего хранил их на флеш-носителе. Виновный незаконно использовал объекты авторского права, а именно, осуществил продажу данных экземпляров программных продуктов. За установку и последующую активацию указанных программных продуктов виновный получил денежное вознаграждение в размере 1500 рублей. Действия были квалифицированы судом по ч. 2 ст. 146 УК РФ, а также по ч. 2 ст. 272 УК РФ.[23]

Приговором Лысковского районного суда Нижегородской области от 2

[22] Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 81.

[23] Приговор Советского районного суда г. Томска от 08.02.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

ноября 2018 г. по делу № 1-108/2018 установлено, что в марте 2018 года, в рабочее время виновному, который работал в офисе ПАО «МТС», неустановленное следствием лицо предложило передавать сведения о входящих и исходящих вызовах абонентских номеров за денежное вознаграждение, на что тот согласился. Так виновный передал указанную, охраняемую законом информацию, к которой осуществил неправомерный доступ, неустановленному лицу, за что получил денежное вознаграждение в сумме 3000 рублей, которые ему перечислило неустановленное лицо. Таким образом виновный совершил преступления, предусмотренные ч. 2 ст. 138, ч. 3 ст. 272, то есть нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений граждан, а также неправомерный доступ к компьютерной информации, с использованием своего служебного положения.[24]

По нашему мнению, дополнительный факультативный объект данного преступления предусмотрен в ч. 3 ст. 272 УК РФ, а именно интересы государственной службы и службы в коммерческих и иных организациях. Также, дополнительный факультативный объект предусмотрен в ч. 4 ст. 272 УК РФ, и определяется в зависимости от вида наступивших тяжких последствий, а также последствий, которые могли наступить вследствие совершения преступления. Иные объекты, которым причиняется вред при совершении преступления, предусмотренного ст. 272 УК РФ не являются дополнительными по отношению к нему, носят самостоятельный характер, и такие деяния квалифицируются по совокупности.

Под предметом преступления принято понимать вещи материального мира, нематериальные ценности и блага, обладающие свойством удовлетворять потребности, воздействуя на которые причиняется вред общественным отношениям, охраняемым уголовным законом.[25]

Б.С. Никифоров определяет предмет преступления как элемент

---

[24] Приговор Лысковского районного суда Нижегородской области от 02.11.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[25] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 106.

нормального правомерного общественного отношения, воздействуя на который, лицо нарушает либо пытается нарушить охраняемое законом общественное отношение.[26]

Некоторые ученые включают в предмет преступления, как материальные объекты, так и нематериальные.

Так, А.И. Рарог понимает предмет преступления как физический предмет материального мира или интеллектуальную ценность, на которые оказывается непосредственное воздействие при совершении преступления.[27]

Предметом неправомерного доступа к компьютерной информации является охраняемая законом компьютерная информация.

Согласно примечанию к ст. 272 УК РФ под компьютерной информацией понимаются сведения, представленные в форме электрических сигналов, независимо от средств их хранения обработки и передачи.

Ранее, определение компьютерной информации содержалось в диспозиции ст. 272 УК РФ, согласно которой компьютерной информацией являлась информация на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети.

С принятием Федерального закона от 07.12.2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации», определение термина «компьютерная информация» изменилось.[28]

Сравнивая определения, можно сделать вывод, что законодатель отказался от перечисления устройств, на которых расположена информация, указывая на то, что представляет собой компьютерная информация.

А.А. Фатьянов критикует позицию законодателя, поскольку хоть понятия «электронно-вычислительная машина» и «ЭВМ» вышли употребления, в

---

[26] Никифоров Б. С. Объект преступления по советскому уголовному праву [Электронный ресурс] / Б. С. Никифоров // Правоведение. – 1962. – № 1. Режим доступа: http://www. law.edu.ru.

[27] Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 83.

[28] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации. [Электронный ресурс] : федер. закон от 07.12.2011 № 420-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

настоящее время используется термин «компьютер». Поэтому, из определения не стоило исключать понятие материального носителя информации, следовало лишь изменить термин. Так, автор пишет о том, что с технической точки зрения, компьютерная информация в любом случае отображается на каком-либо машинном носителе (микросхема, либо намагниченная поверхность рабочего тела, то есть жесткого диска компьютера – основного хранителя программной и пользовательской информации). [29]

О необходимости введения нового определения понятия, которое отражало бы нахождение информации на материальном носителе, пишут А.Н. Тарбагаев, А.В. Суслопаров. Так, в своей работе, они предлагают внести термин «компьютер» или «компьютерная система», понимая под ними устройство или группу взаимосвязанных устройств, осуществляющих обработку данных.[30]

М.А. Ефремова поддерживает позицию законодателя. Действительно, «компьютер» – это технический термин. Законодатель, используя технические термины в Особенной части УК РФ, создает трудности для правоприменения. Так, согласно ее утверждениям, появление новых средств хранения, передачи и обработки информации и их усовершенствование процесс динамичный. В настоящее время компьютерная информация хранится и обрабатывается в технических устройствах, которые в прямом значении не являются компьютерами, но имеют некоторые схожие с компьютерами свойства или же компьютер это средство управления работой такого устройства.[31]

По нашему мнению, вводить в определение понятие «компьютерная информация» нахождение информации на каком-либо материальном носителе нецелесообразно, поскольку компьютер не единственное средство хранения и

---

[29] Фатьянов А. А О дефиниции «компьютерная информация» в российском уголовном законодательстве [Электронный ресурс] / А. А. Фатьянов // Информационное право. – 2017. – № 3. – Режим доступа: http://cyberleninka.ru

[30] Тарбагаев А. Н. Ответственность за неправомерный доступ к компьютерной информации: уголовно-правовой и административно-правовой аспект [Электронный ресурс] / А. Н. Тарбагаев, А. В. Суслопаров // Вестник Омского университета. –2012. – № 2. – Режим доступа: http://www.cyberleninka.ru

[31] Ефремова А. М. К вопросу о понятии компьютерной информации [Электронный ресурс] / А. М. Ефремова // Юрист. – 2012. – № 1. – Режим доступа: http://www.consultant.ru.

обработки информации, а перечислить все средства невозможно. Так материальных носителей информации достаточно много, и при появлении новых средств хранения и обработки информации возникнет необходимость во внесении изменений в УК РФ.

Существуют доктринальные определения понятия «компьютерная информация».

Так, А.В. Суслопаров определяет компьютерную информацию как сведения, которые не могут иметь каких-либо физических характеристик, хранящиеся на материальном носителе. Такие сведения передаются между субъектами в форме электронного кода с помощью сигналов.

Он перечисляет признаки компьютерной информации:

1. информация должна передаваться посредством сигнала;

2. форма информации представлена определенным кодом;

3. информация не имеет каких-либо физических характеристик;

4 информация может быть преобразована новую информацию;

5. признаки информации можно проследить только при наличии совокупности субъекта, объекта, предатчика, канала, приемника а также источника помех.[32]

В соответствии с легальным определением, компьютерная информация – это сведения.

Легальное определение информации содержится в ст. 2 Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации». Под информацией понимаются сведения (сообщения, данные) независимо от формы их представления.[33]

Таким образом, сведения составляют сообщения и данные.

А.А. Нагорный в своей работе дает определение сообщения. Сообщение – это форма представления информации в виде текстов, схем, различных

---

[32] Суслопаров А. В. Информационные преступления : автореф. дис….канд. юридических наук : 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2008. 24 с.

[33] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

графических изображений. Сообщение будет являться информацией лишь при наличии потенциального потребителя, воспринимающего субъекта.[34]

Легальное определение данных содержится в ст. 1 Конвенции о киберпреступности. Под данными в ней понимается любое представление информации, фактов, идей в форме, пригодной для обработки в компьютерной системе, включая программу, которая предназначена для функционирования компьютерной системы.[35]

В свою очередь, в информатике, под данными можно понимать информацию, которая закодирована с целью хранения, передачи и обработки, а также ее поиска. Другими словами, формой представления информации на материальном носителе являются данные. Данные не подразумевают наличие адресата, в отличии от сообщений, для которых предусмотрен определенный получатель.[36]

В своей работе А.Н. Тарбагаев, А.В. Суслопаров предлагают заменить в статье 272 УК РФ компьютерную информацию на данные. Авторы считают наиболее удачным использование термина данные, поскольку он акцентирует внимание на форме существования информации.[37]

Второй признак компьютерной информации – сведения должны быть представлены в виде электрических сигналов.

Под сигналом понимается материальный носитель информации, который используется для передачи сообщений. В науке существует дискуссия относительно понятия электрический сигнал. Так, в соответствии с теорией таких наук как физика и информатика, вся информация, содержащаяся и обрабатываемая компьютером, должна быть представлена двоичным кодом (с

---

[34] Нагорный А.А. Содержание понятия «компьютерная информация» как предмета компьютерных преступлений [Электронный ресурс] / А.А. Нагорный // Актуальные проблемы российского права. – 2014. – № 1. – Режим доступа: http://www.consultant.ru.

[35] Европейская конвенция по киберпреступлениям от 21.11.2001. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[36] Мицкевич А. Ф. Понятие компьютерной информации по российскому и зарубежному уголовному праву [Электронный ресурс] / А. Ф.Мицкевич, А. В. Суслопаров // Пробелы в российском законодательстве. Юридический журнал. –2010. – № 2. – Режим доступа: http://www.cyberleninka.ru.

[37] Тарбагаев А. Н. Ответственность за неправомерный доступ к компьютерной информации: уголовно-правовой и административно-правовой аспект [Электронный ресурс] / А. Н. Тарбагаев, А. В. Суслопаров // Вестник Омского университета. –2012. – № 2. – Режим доступа: http://www.cyberleninka.ru

помощью цифр 0 и 1). По мнению М.А. Ефремовой, информация, которая передается по беспроводным и оптическим каналам связи, согласно данной норме, не подлежит уголовно-правовой охране, поскольку такая информация не охватывается определением электрических сигналов (если определять данный термин с точки зрения информатики и физики). Следовательно, автор считает, что использование в уголовном законе термина «электрический сигнал», создает проблемы в его трактовке правоприменителем, поскольку точно не определен и поэтому нуждается в разъяснении или замене.[38]

Так, М.А. Ефремова предлагает отказаться от термина «электрический сигнал».

Более того, автор предлагает заменить термин «компьютерная информация» на схожее, однако отличающееся по значению понятие «электронная информация». В случае таких изменений, под электронной информацией необходимо понимать электронно-цифровые сведения. При этом не имеет значение вид средства хранения этих сведений, их обработки и передачи.[39]

А.А. Фатьянов также утверждает, что далеко не все электрические сигналы являются компьютерной информацией. Так, электрический сигнал может и не нести в себе полезной для конкретного субъекта информации, но при этом по своей физической природе не перестает быть электрическим сигналом.[40]

Верховный Суд Российской Федерации, в официальном отзыве от 7 апреля 2011 г. № 1/общ-1583 «На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» отмечает, что предложенный в примечании к ст. 272

[38] Ефремова А. М. К вопросу о понятии компьютерной информации [Электронный ресурс] / А. М. Ефремова // Юрист. – 2012. – № 1. – Режим доступа: http://www.consultant.ru.
[39] Там же.
[40] Фатьянов А.А. О дефиниции «компьютерная информация» в российском уголовном законодательстве [Электронный ресурс] / А.А. Фатьянов // Информационное право. – 2017. – № 1. – Режим доступа: http://www.consultant.ru.

УК РФ термин «электрический сигнал» недостаточно определен и требует дополнительных разъяснений.[41]

Также, В заключении Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05.07.2011, было отмечено, что «в предлагаемой дефиниции не ясен смысл термина «электрические сигналы».[42]

Пункт «б» ст. 1 Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г. определяет компьютерную информацию как информацию, находящуюся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи.[43]

Действительно, следует заметить, что термин «электрические сигналы» не имеет точного определения. Требуются разъяснения по поводу того, в каком смысле законодатель употребляет термин «электрические сигналы», а также какие сигналы следует относить к электрическим.

Однако соглашаться с позицией, выраженной в Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 г., которое определяет компьютерную информацию как информацию, находящуюся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи, также нельзя, поскольку в данном случае указывается на нахождение информации на различных видах материальных носителей.

---

[41] На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» [Электронный ресурс] : Официальный отзыв ВС РФ от 7.04.2011 г. № 1/общ-1583 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[42] На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ» (к первому чтению) [Электронный ресурс] : Заключение Комитета по информационной политике, информационным технологиям и связи от 05.07.2011 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[43] Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

По нашему мнению, следует согласиться с точкой зрения А.М. Ефремовой и отказаться от указания на «электрические сигналы», поскольку разъяснение технических терминов в законодательстве создаст еще больше трудностей в применении нормы. Так, под компьютерной информацией должны пониматься сведения, представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи.

В статье 272 УК РФ указано, что доступ должен быть осуществлен именно к компьютерной информации, охраняемой законом. Следует отметить, что охраняется только та совокупность общественных отношений по правомерному и безопасному использованию, которая находится под защитой закона. Следовательно, охраняемая законом компьютерная информация – это информация с ограниченным доступом, имеющая специальный правовой статус, а также предназначена для ограниченного круга лиц, имеющих право на ознакомление с ней.

Информация признается охраняемой законом при соблюдении нескольких условий.

Во-первых, закон ставит под защиту информацию от неправомерного доступа.

Так, особый режим охраны установлен для сведений, составляющих государственную тайну (ФЗ РФ от 21.07.1992 № 5485-1 «О государственной тайне»), банковскую тайну (ст. 857 ГК РФ, ФЗ № 395-1 от 02.12.1990 «О банках и банковской деятельности»); тайну исповеди (ФЗ от 26.09.1997 № 125-ФЗ «О свободе совести и религиозых объединениях»), аудиторскую тайну (ФЗ от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности») и др.

Также, в соответствии со статьей 9 Федерального закона № 152-ФЗ от 27.07.2006 «О персональных данных», субъект персональных данных принимает решение о предоставлении его персональных данных и дает согласие на их обработку, своей волей и в своем интересе. Согласие на

обработку персональных данных должно быть конкретным, информированным и сознательным.[44]

Таким образом, без согласия лица на обработку такой информации, доступ к ней ограничен.

Согласно ч. 3 ст. 4 Федерального закона № 98-ФЗ от 29.07.2004 «О коммерческой тайне», информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом.[45]

Таким образом, вышеуказанная информация также является охраняемой законом.

Так, приговором Мотовилихинского районного суда г. Перми от 25 февраля 2019 г. по делу № 1-73/2019 установлено, что виновные, осознавая, что получение и разглашение сведений, составляющих коммерческую тайну, без согласия их владельца, а также неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование, запрещены на территории Российской Федерации действующим законодательством, имея умысел на незаконное обогащение и получение постоянного незаконного источника доходов за счет средств, добытых преступным путем, в составе организованной группы, совершили преступления, связанные с получением и разглашением сведений, составляющих коммерческую тайну, без согласия их владельца, а также с неправомерным доступом к охраняемой законом компьютерной информации, повлекшим ее копирование. Действия лиц были квалифицированы по ч. 3 ст. 183, а также по ч. 3 ст. 272 УК РФ.[46]

---

[44] О персональных данных. [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

[45] О коммерческой тайне. [Электронный ресурс] : федер. закон от 29.07.2004 № 98-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru

[46] Приговор Мотовилихинского районного суда г. Перми от 25.02.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

Вторым условием, при котором компьютерная информация может считаться охраняемой законом – принятие законным обладателем информации каких-либо мер по ее охране.[47]

В Федеральном законе от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», видами информации являются общедоступная и информация, доступ к которой ограничен. Критерий разграничения – возможность доступа к ней. Согласно ст. 7 ФЗ № 149 к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. Таким образом, исходя из вышесказанного, необходимо указать на признаки общедоступной информации. Из них – отсутствие ограничений и запретов на доступ к информации, а также общеизвестность.

Пунктом третьим ст. 3 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», установлено, что право обладателя информации разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа.[48]

Следовательно, признаком «охраняемая законом» информация обладает в следующих случаях. Во-первых, определения порядка доступа к ней либо ограничение доступа иных лиц к информации. Во-вторых, в случаях нереализации такого права обладателем информации, соответственно и вышеназванным признаком она не обладает.[49]

Также следует отметить, что общедоступная информация не всегда является не охраняемой законом. По смыслу ст. 7 Федерального закона «Об информации» общедоступность информации подразумевает ее свободное распространение, а не осуществление других действий. Так, по мнению Р.И. Дремлюга, общедоступность информации, подразумевает только доступ на ее

---

[47] Новое в Уголовном кодексе (постатейный) [Электронный ресурс] / под ред. А. И. Чучаева. – Режим доступа: http://www.consultant.ru.

[48] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[49] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

копирование, а не на остальные действия, упомянутые в ст. 272 УК РФ. Следовательно, нельзя исключать общедоступную информацию из предмета преступления, предусмотренного ст. 272 УК РФ.[50]

В научной литературе высказывается мнение о существовании дополнительного признака компьютерной информации – ценность информации.

А.И. Куприянов и В.В. Шевцов определяют ценность информации как максимальную пользу, которую может принести данное количество информации, или как те максимальные потери, к которым приведет утрата этого количества информации.[51]

Однако такая точка зрения вызывает споры в науке. В.Г. Степанов-Егиянц полагает, что понятие «ценность информации» является оценочным и ее должен определять обладатель такой информации.[52]

По нашему мнению, ценность информации значение не имеет, не зависит от ее оценки правообладателем, и, следовательно, не влияет на квалификацию деяния.

Некоторые ученые предлагают расширить предмет преступления, предусмотренного ст. 272 УК РФ.

Существует позиция, согласно которой к предмету неправомерного доступа к компьютерной информации необходимо отнести технические устройства, на которых эта информация хранится.

Так, В.С. Комиссаров считает, что предметом любого компьютерного преступления следует признать компьютер как носитель информации.[53]

Ю.В. Гаврилин пишет о том, что компьютер не может являться предметом данного преступления. Данный вывод он обосновывает примером,

---

[50] Дремлюга Р. И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ [Электронный ресурс] / Р. И. Дремлюга // Уголовное право. – 2018. – № 4. – Режим доступа: http://www.consultant.ru.

[51] Куприянов А.И. Оптимизация мер по защите с учетом ценности информации [Электронный ресурс] / А.И. Куприянов, В.В. Шевцов – М.: Известия института инженерной физики. – 2012. – № 25. – Режим доступа: http://www.elibrary.ru.

[52] Степанов-Егиянц, В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[53] Российское уголовное право. Общая часть : учебник для вузов / под ред. В.С. Комиссарова. – М.: Статут, 2012. – Режим доступа: http://www.consultant.ru.

так, при повреждении компьютера или другого технического устройства либо его завладением, удаление содержащейся в нем информации не может являться составом данного преступления. Такое деяние, может признаваться преступным в сфере отношений против собственности.[54]

А.В. Суслопаров считает данную позицию ошибочной, поскольку компьютерная информация не имеет материальной формы и не зависит от материального носителя.[55]

По нашему мнению, стоит согласиться с мнением А.В. Суслопарова, и понимать под предметом данного преступления компьютерную информацию, вне зависимости от средств ее хранения, поскольку повреждение материального носителя информации нарушает иные правоотношения, защита которых не предусмотрена ст. 272 УК РФ.

В науке также отмечается возможность признания предметом преступления информационную среду, под которой понимается деятельность субъектов, связанная с созданием, преобразованием и потреблением информации.[56]

По нашему мнению, ст. 272 УК РФ предусматривает ответственность за неправомерный доступ именно к компьютерной информации. Предмет данного преступления не может сводиться к средствам хранения информации либо деятельности субъектов. Такая позиция авторов необоснованно расширяет предмет преступления, предусмотренного ст. 272 УК РФ и может привести к ошибкам в квалификации.

Таким образом, в настоящее время под предметом неправомерного доступа к компьютерной информации понимается охраняемая законом компьютерная информация, то есть сведения, передающиеся между субъектами посредством электрических сигналов, независимо от средств хранения, обработки и передачи.

---

[54] Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации [Электронный ресурс] : учеб. пособие: / под ред. Н.Г. Шурухнова. М.: ЮИ МВД РФ; Книжный мир, 2001. – Режим доступа: http://www.law.edu.ru.

[55] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[56] Там же.

1.2 Объективная сторона неправомерного доступа к компьютерной информации

Объективная сторона – система признаков, определяющих уголовно-правовое значение общественно опасного деяния как внешнего события или внешней деятельности субъекта.[57]

Эти признаки образуют систему, которая состоит из нескольких элементов, таких как деяние, последствия, причинная связь. А также факультативных элементов: места, времени, способа, обстановки и иных внешних обстоятельств.[58]

Общественно-опасное деяние – сознательное и волевое внешнее поведение человека.[59]

Определение объективной стороны неправомерного доступа к компьютерной информации содержится в дефиниции ст. 272 УК РФ. Так деянием будет являться «неправомерный доступ» к охраняемой законом компьютерной информации.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», под доступом понимается проникновение в ее источник с использованием средств (вещественных и интеллектуальных) компьютерной техники, позволяющее использовать полученную информацию (копировать, модифицировать, блокировать либо уничтожать ее).[60]

Статья 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об

---

[57]Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 94.
[58]Там же.
[59]Там же.
[60]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

информации, информационных технологиях и о защите информации», определяет доступ к информации как возможность получения информации и ее использования. Под «использованием», в Законе, понимается распространение информации по своему усмотрению, то есть осуществление действия, направленного на получение информации неопределенным кругом лиц и передачу информации неопределенному кругу лиц.[61]

В доктрине также существуют мнения по поводу определения понятия «доступ».

«Доступ», по мнению А.Г. Волеводза, некий способ проникновения в средства хранения информации (ее источник), такое активное действие, при помощи которого лицо получает информацию. Форма такого проникновения включает в себя несколько различных способов. Проникновение в источник позволяет субъекту доступа определенным образом осуществлять воздействие на информацию. Видами воздействия можно назвать копирование, блокирование, модификацию и уничтожение компьютерной информации. Совершить доступ бездействием не представляется возможным.[62]

По мнению В. Г. Степанова-Егиянца, под доступом к компьютерной информации следует понимать получение возможности обращения к компьютерной информации, результатом которого является получение лицом правомочия обладателя информации.[63]

Для правильной квалификации необходимо определить момент начала и окончания доступа.

Так, в своей работе В.К. Гавло, В.В. Поляков определяют момент начала деяния с момента начала воздействия на информацию в объекте преступного

---

[61]Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[62]Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Электронный ресурс] : монография / А. Г. Волеводз – Москва : Юрлитинформ, 2011. – Режим доступа: http:// www.mgimo.ru.

[63]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

посягательства.[64]

По нашему мнению, данная позиция не является верной.

Момент начала выполнения объективной стороны неправомерного доступа к охраняемой законом компьютерной информации, по мнению А.Ю. Решетникова, Е.А. Русскевича определяется осуществлением лицом действий, которые непосредственно направлены на преодоление средств защиты информации и их нейтрализацию.[65]

Так, можно выделить стадии совершения неправомерного доступа. Приготовлением к преступлению будут являться такие действия как получение логинов и паролей, планирование технической стороны совершения преступления, подыскание специализированных программ для доступа. Покушением можно признать действия, непосредственно направленные на получение доступа, ввод паролей, использование программ для получения доступа к информации и другие. Начало деяния связано с совершением данных действий.

Моментом окончания доступа будет считаться получение доступа к компьютерной информации, когда лицо имеет возможность осуществлять манипуляции с информацией и воздействовать на нее.

Согласно ст. 272 УК РФ доступ должен быть неправомерным.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», неправомерным считается доступ к конфиденциальной информации или информации, составляющей государственную тайну, лица, не обладающего необходимыми полномочиями (без согласия собственника или его законного представителя), при условии обеспечения специальных средств ее защиты.

---

[64] Гавло В.К. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации [Электронный ресурс] / В.К. Гавло, В.В. Поляков // Известия государственного Алтайского университета. – 2006. – № 2. – Режим доступа: http://www.consultant.ru.

[65] Решетников А.Ю. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации [Электронный ресурс] / А.Ю. Решетников, Е.А. Русскевич // Уголовное право. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

Другими словами, неправомерный доступ к компьютерной информации – это незаконное либо не разрешенное собственником или иным ее законным владельцем использование возможности получения компьютерной информации.[66]

В. Г. Степанов-Егиянц, однако, полагает, что доступ является неправомерным в случае, когда лицом допущено нарушение при обращении с информацией, а именно нарушен порядок доступа, либо осуществлено такое действие вопреки воле владельца информации, при попытке воздействия на информацию.[67]

Дискуссионным является вопрос относительно того, должна ли компьютерная информация находиться под какой-либо защитой.

В. Г. Степанов-Егиянц считает, что отсутствие защиты данных, находящихся на компьютере, не означает, что доступ к этой информации не будет являться преступлением.

Автор полагает, что определяющие критерий при квалификации данных преступных деяний – использование исключительного права на ограниченный доступ к информации, а не применение средств защиты. Ученый считает, что если информация находится на материальном носителе, в том числе и компьютере без средств защиты, то в таком случае доступ также будет неправомерным.[68]

По нашему мнению, неправомерным доступ также считается тогда, когда он осуществляется лицом, которое не обладает необходимыми полномочиями (без согласия собственника или его законного представителя), не зависимо от того установлены средства защиты информации или нет.

Таким образом, неправомерным доступом к компьютерной информации необходимо признать действия, связанные с попыткой получить возможность

---

[66]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[67]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[68]Там же.

воздействия на информацию, либо получение возможности использовать, либо обратится к такой информации, которое осуществляется без надлежащего разрешения, с дефектным разрешением, либо с выходом за пределы полученного разрешения.

Общественно-опасное последствие – это такое вредное изменение в объекте уголовно-правовой охраны, которое предусмотрено УК РФ, и наступает или может наступить в результате совершения преступления.[69]

Данный состав преступления носит материальный характер и предполагает обязательное наступление одного или нескольких указанных в законе последствий.[70]

Статья 272 УК РФ предусматривает как одно из последствий данного преступления – уничтожение охраняемой законом компьютерной информации.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления.[71]

В доктрине считается спорным вопросом о том, что считать уничтожением.

А. В. Степанов-Егиянц, утверждает, что знаний о наличии у обладателя компьютерной информации ее копии, либо о технической, либо иной возможности восстановить информацию, при совершении неправомерного доступа к компьютерной информации у лица быть не может и не должно быть, поскольку для квалификации это значение не имеет. Единственное, что в данном случае должно иметь значение для правильной квалификации деяния,

---

[69]Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. С. 102.

[70]Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [Электронный ресурс] / под ред. В. М. Лебедева. – Режим доступа: http://www.consultant.ru.

[71]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

это направленность умысла субъекта преступления. Приводя пример, автор указывает, что уничтожив компьютерную информацию, имея заранее намерение на ее уничтожение, деяние подлежит квалификации по ст. 272 УК РФ, несмотря на то, что информация может быть восстановлена.[72]

А. Г. Волеводз считает, что при уничтожении информации преступление считается оконченным, если данная информация восстановлению не подлежит.[73]

У. В. Зинина полагает, что если есть возможность восстановить информацию, то такое деяние должно признаваться покушением на преступление, предусмотренное ст. 272 УК РФ.[74]

Проанализировав судебную практику, можно сделать вывод о том, что суды руководствуются методическими рекомендациями при разрешении дел.

Так, приговором Советского районного суда г. Казани № 1-212/2018 от 15 мая 2018 г. установлено, что лицо, обладая определенными знаниями и необходимыми навыками в сфере информационных технологий, проник в офис организации, и преследуя прямой преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации и ее уничтожение, воспользовавшись приготовленным флеш-накопителем, совершил неправомерный доступ и уничтожение с компьютера сведений, необходимых для осуществления деятельности организации (транспортные услуги и продажа запчастей для спецтехники). Данные сведения включали объекты интеллектуального труда – материалы по диссертации, сведения об именах и наименованиях заказчиков (реквизиты, контакты, данные руководителей). При этом суд указал, что под уничтожением информации следует понимать приведение информации или ее части в непригодное для использования состояние, независимо от возможности ее восстановления.

---

[72]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.
[73]Волеводз А. Г. Указ. соч. – Режим доступа: http:// www.mgimo.ru.
[74]Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве [Электронный ресурс]: Дис. ... канд. юрид. наук. : 12.00.08 / Зинина Ульяна Викторовна. – Москва , 2007. – Режим доступа: http://www. diss.seluk.ru.

Таким образом, лицо было признано виновным в совершении преступления, предусмотренного ч. 1 ст. 272 УК РФ.[75]

По нашему мнению, нельзя говорить об уничтожении информации, если имеется возможность ее восстановить, поскольку если информация восстанавливаема, то она не уничтожена, а значит, вред объекту не причиняется.

Также, необходимо отметить следующее. В случае, когда информация не уничтожена, но осуществлены иные действия, не влияющие на содержание информации и иные ее признаки, к примеру, переименование, перемещение в другое место на материальном носителе, то такое деяние, осуществленное в результате неправомерного доступа к компьютерной информации следует квалифицировать не как уничтожение данной информации, а как блокирование либо модификацию (зависит от обстоятельств конкретного преступления).[76]

А также само по себе автоматическое «вытеснение» старых версий файлов последними по времени не будет являться уничтожением.[77]

Таким образом, под уничтожением следует понимать приведение информации или ее части в непригодное для использования состояние при котором восстановить информацию невозможно.

Следующим последствием неправомерного доступа к компьютерной информации является блокирование такой информации.

«Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации» определяют блокирование как результат воздействия 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, то есть совершение действий, приводящих к

---

[75] Приговор Советского районного суда г. Казани № 1-212/2018 от 15 мая 2018 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.
[76]Волеводз А. Г. Указ. соч. – Режим доступа: http:// www.mgimo.ru.
[77]Степанов-Егиянц В. Г. Указ.соч. – Режим доступа: http://www.consultant.ru.

ограничению или закрытию доступа к компьютерному оборудованию и находящимся на нем ресурсам, целенаправленное затруднение доступа законных пользователей к компьютерной информации, не связанное с ее уничтожением.[78]

Для определения понятия блокирования необходимо обратится к ГОСТу Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения». В п. 3.3.8 указано, что, блокирование доступа к информации – прекращение доступа к информации законных пользователей, а также затруднение доступа к информации этим лицам.[79]

В соответствии с позицией Л.М. Болсуновской, существуют такие признаки блокирования компьютерной информации как: невозможность постоянного или временного получения доступа к компьютерной информации; «блокирование» не должно повлечь изменения содержания информации, информация остается нетронутой, однако становится недоступной.[80]

По мнению В. Г. Степанова-Егиянца, для вменения признака блокирование компьютерной информации, необходимо чтобы такое блокирование продолжалось определенное время, которое необходимо для нарушения возможности пользователя обращаться к информации и использовать информацию. Либо такое деяние должно создать угрозу нарушения возможности пользователя осуществлять работу с информацией.[81]

По нашему мнению блокирование информации, длящееся непродолжительное время, не повлекшее негативных последствий для собственника информации, не может признаваться преступлением. При неправомерном доступе к компьютерной информации, повлекшее ее

---

[78]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[79]ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения – Москва : Стандартинформ, 2009.

[80]Болсуновская Л.М. Анализ способов совершения мошенничества в сфере компьютерной информации [Электронный ресурс] / Л. М. Болсуновская // Проблемы экономики и юридической практики. – 2015. – № 2. – Режим доступа: http://www.consultant.ru.

[81]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

блокирование важно учитывать, что такое блокирование должно нарушить нормальную работу обладателя информации и влечь для него негативные последствия.

Приговором Балтийского городского суда № 1-12/2019 от 19 февраля 2019 г., установлено, что, лицо, являлось обучающимся работником по договору об обучении заключенным с организацией. Данным договором лицу был вверен рабочий компьютер, который позволял осуществлять обращение к базе клиентов – абонентов при помощи пароля. Находясь на рабочем месте и используя пароль от программы с клиентской базой (принадлежавший его руководителю), имея корыстные побуждения и умысел, осуществил блокирование для абонента доступа к подключенным им услугам, и таким образом осуществил блокирование компьютерной информации. Затем виновный восстановил заблокированную сим-карту и продал ее иному лицу – клиенту, с абонентским номером предыдущего владельца, таким образом осуществил модификацию компьютерной информации.[82]

Указанные выше действия квалифицированы по ч. 3 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, повлекший блокирование и модификацию компьютерной информации, совершённый из корыстной заинтересованности лицом с использованием своего служебного положения.

Таким образом, блокирование – это результат воздействия на компьютерную информацию или технику, последствием которого является нарушение нормальной работы с информацией ее обладателем, невозможность в течение некоторого времени или постоянно осуществлять требуемые операции над компьютерной информацией полностью или в требуемом режиме, не связанное с ее уничтожением.

Также одним из последствий данного преступления является модификация охраняемой законом компьютерной информации.

[82] Приговор Балтийского городского суда № 1-12/2019 от 19 февраля 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», модификация информации – это внесение изменений в компьютерную информацию (или ее параметры).[83]

А. Г. Волеводз определяет модификацию как внесение изменений в программы, базы данных, текстовую и любую другую информацию, находящуюся на материальном носителе, кроме ее легальной модификации.[84]

Легальной модификацией программ, баз данных (следовательно и информации) лицами, правомерно владеющими этой информацией признаются:

1) модификация в виде исправления явных ошибок;

2) модификация в виде внесения изменений в программы, базы данных для их функционирования на технических средствах пользователя.[85]

М. И. Третьяк определяет термин «модификация» как обобщающий термин, включающий любое воздействие на компьютерную информацию, при котором возможны два результата: появление новой информации или сочетание новой и имеющейся информации.[86]

По нашему мнению, не любое внесение изменений в компьютерную информацию является преступным. Так, изменения, не влекущие негативных последствий для правообладателя, не причиняющие вреда объекту посягательства, не будут являться преступными.

Можно привести примеры из судебной практики квалификации деяния как неправомерный доступ к компьютерной информации, повлекший ее модификацию.

---

[83]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[84]Волеводз А. Г. Указ. соч. – Режим доступа: http:// www.mgimo.ru.

[85]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[86]Третьяк М. И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества [Электронный ресурс] / М. И. Третьяк // Уголовное право. – 2016. – № 2. – Режим доступа: http://www.consultant.ru.

Так, приговором Энгельского районного суда № 1-1-203/2019 1-203/2019 от 21 марта 2019 г., виновный распечатал, а в дальнейшем собственноручно поставил в заявлении подпись от имени абонента, без его фактического обращения. Сведения, внесенные виновным в программное обеспечение в ходе совершения операций по замене сим-карты, в дальнейшем были автоматически выгружены в базу данных, новой сим-карте был присвоен абонентский номер, что повлекло изменение в компьютерной информации, содержащейся в указанной базе данных в части информации об абонентском номере, владельце номера, серийном номере сим-карты. Таким образом, действия виновного привели к модификации компьютерной информации.

Суд квалифицировал действия по ч. 3 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло модификацию компьютерной информации, совершенный лицом с использованием своего служебного положения.[87]

Приговором Советского районного суда г. Орла № 1-43/2019 от 13 июня 2019 г. по делу № 1-43/2019, виновный, бывший сотрудник организации, находясь в здании организации, используя компьютер с доступом в «Интернет», путем создания новой учетной записи (данные которой не установлены) пользователя сайта «regionorel.ru» осуществил неправомерный доступ к компьютерной информации, после чего произвел модификацию компьютерной информации, путем введения в текст имеющегося в его распоряжении кода скрипта с индивидуальным ключом для получения криптовалюты «Monero» в личное пользование. В результате указанные преступные действия виновного повлекли модификацию вышеуказанной охраняемой законом компьютерной информации.

Суд квалифицировал действия по ч. 2 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, если это деяние

[87] Приговор Энгельского районного суда № 1-1-203/2019 1-203/2019 от 21 марта 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

повлекло модификацию компьютерной информации, совершенный из корыстной заинтересованности.[88]

В науке существует дискуссия по поводу подключения к сети Интернет с помощью логинов и паролей, принадлежащих другим лицам. В данном случае нарушаются интересы провайдера, который предоставляет услуги по пользованию сетью Интернет. Так, на серверах, принадлежащим провайдерам изменяется информация, носящая статистический характер (объем предоставляемых услуг конкретному лицу). Ранее в практике такие деяния квалифицировались судами по ст. 272 УК РФ, как неправомерный доступ к компьютерной информации, повлекший ее модификацию.

Ученые по-разному относятся к такой квалификации деяния.

По мнению У.В. Зининой, сведения, которые фиксируются в базах данных провайдера, о фактах неправомерного доступа не являются модификацией охраняемой законом компьютерной информации, поскольку умыслом лица такое изменение не охватывается.[89]

По мнению В. Г. Степанова-Егиянца, лицо, получившее доступ в Интернет при помощи логина и пароля, принадлежащего иному пользователю, совершает преступление, предусмотренное ст. 272 УК РФ. Это связано с модификацией компьютерной информации (с косвенным умыслом) вследствие внесения изменений в различные данные провайдера и его статистику. Помимо этого исследователь подчеркивает, что под понятие охраняемая законом информация попадают регистрационные данные. Следовательно, квалификация доступа по ст. 272 УК РФ неизбежна.[90]

Так, согласно приговору Оренбургской области от 27.02.2011 № 1-55/2011 неправомерный доступ к компьютерной информации привел к модификации охраняемой законом компьютерной информации, что повлекло

---

[88] Приговор Советского районного суда г. Орла № 1-43/2019 от 13 июня 2019 г. [Электронный ресурс]. – Режим доступа: http://www.sudact.ru.

[89]Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве [Электронный ресурс] : дис. ... канд. юрид. наук.: 12.00.08/ Зинина Ульяна Викторовна. – Москва , 2007. – Режим доступа: http://www. diss.seluk.ru.

[90]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

изменение статистических данных о пользователе, времени начала и продолжительности работы, количестве соединений, поступающих на сервер статистики Оренбургского филиала ОАО. Суд квалифицировал деяние по ч. 1 ст. 272 УК РФ, то есть как неправомерный доступ к охраняемой законом компьютерной информации, повлекший модификацию компьютерной информации.[91]

По нашему мнению, такие деяния не будут являться преступными, поскольку не причиняют вреда объекту преступного посягательства, и не нарушают нормальную работу интернет провайдера.

Таким образом, модификацией признается изменение (внесение новой информации, ее частичная замена, изменение ее первоначального вида, не меняющая ее сущность) первоначальной информации без согласия собственника или иного законного владельца. При этом количество возможных вариантов таких изменений практически не ограничено.

Одним из признаков образующих объективную сторону преступления, предусмотренного ст. 272 УК РФ является наступление последствия в виде копирования охраняемой законом компьютерной информации.

При этом анализ судебной практики за 2015-2020 гг. показывает, что последствие в виде копирования является самым распространенным при совершении преступлений, предусмотренных ст. 272 УК РФ. Данный признак вменяется виновным более чем в 50% случаев вынесения обвинительных приговоров.

Однако следует отметить, что точного определения данного признака в законе не дано, поэтому отсутствует единообразное толкование понятия копирования в науке и судебной практике.

В соответствии с «широким» подходом, копирование компьютерной информации представляет собой любое ее воспроизведение или тиражирование. Под копированием понимают:

---

[91]Приговор Промышленного районного суда г.Оренбурга от 27.02.2011 № 1-55/2011 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

Во-первых, тираж путем печати[92], «ознакомление с экрана технического устройства»[93], «переписывание, иное размножение». А во-вторых, разглашение, воспроизведение подлинного или относительно подлинного ее оригинала». Под копированием необходимо понимать воспроизведение или запись охраняемой законом компьютерной информации на ином носителе, не являющемся исходным.[94]

М. А. Зубова считает, что копирование может осуществляться не только переносом на другой машинный носитель, но и ее воспроизведение в любой материальной форме, к примеру, переписывание, фотографирование с экрана компьютера, ознакомление с информацией на экране.[95]

Подобное понимание копирования можно встретить и в некоторых официальных источниках.

Так, согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», копирование информации – создание копии имеющейся информации на другом носителе, то есть перенос информации на обособленный носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме – от руки, фотографированием текста с экрана дисплея, а также считывания информации путем любого перехвата информации и т.п.[96]

П. 1 «Справки Верховного Суда Республики Крым по результатам изучения судебной практики по уголовным делам о преступлениях в сфере компьютерной информации (гл. 28 УК РФ)» определяет копирование

---

[92] Полубинская С. В. Учебный комментарий к уголовному кодексу Российской Федерации / под ред. М. Жалинского – Москва : Эксмо, 2005. С. 837.

[93] Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дисс … канд. юр. наук : 12.00.08 / Малыковцев Михаил Михайлович. – М., 2006. С. 108.

[94] Ефремова Т. Ф. Новый словарь русского языка. Толково-образовательный. / Т. Ф. Ефремова – Москва : Русс. Яз., 2000. в 2-х т. С. 1209.

[95] Зубова М. А. Неправомерный доступ к компьютерной информации и его последствия [Электронный ресурс] / М. А. Зубова // Бизнес в законе. Экономико-юридический журнал. – 2007. – № 3. Режим доступа: http://www.cyberleninka.ru.

[96] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

информации как создание копии имеющейся информации на другом носителе, то есть перенос на другой обособленный от ЭВМ носитель при сохранении неизменной первоначальной информации, воспроизведение информации в любой материальной форме: от руки, путем фотографирования текста с экрана дисплея.[97]

Такой подход, по нашему мнению, необоснованно расширяет понятие копирования информации, что делает его непригодным для правоприменения. В данном случае в первую очередь нарушается конфиденциальность информации (ознакомление с нею). Последствием этого является копирование посредством воспроизведения на различных материальных носителях (переписывание собственноручно с экрана технического устройства на лист бумаги и.т.д.). Кроме того, при таком подходе фактически ставится знак равенства между копированием информации и считыванием информации (ознакомлением с ней). Такое понимание копирования не соответствует этимологическому значению понятий «копия», «копирование». Копия представляет собой объект, созданный по образцу другого, повторяющий, воспроизводящий его внешний вид и другие свойства. Это точно соответствующее подлиннику воспроизведение чего-либо.[98] Соответственно копия в смысле ст. 272 УК РФ должна иметь форму, соответствующую предмету преступления, то есть быть именно компьютерной информацией, которая остается на различных носителях информации.

Следовательно, наиболее предпочтительным следует признать «узкое» понимание копирования информации, то есть создание идентичной копии на машинном носителе.

Вторая группа исследователей допускает копирование только в форме «… создания идентичной последовательности байтов»[99]. Так, в данном случае

---

[97] Справка Верховного Суда Республики Крым по результатам изучения судебной практики по уголовным делам о преступлениях в сфере компьютерной информации (гл. 28 УК РФ) [Электронный ресурс]. – Режим доступа: http://www.consultant.ru.

[98] Ефремова Т. Ф. Новый словарь русского языка. Толково-образовательный.: в 2-х т. / Т. Ф. Ефремова – Москва : Русс. Яз., 2000. Т. 1. С. 1209.

[99] Крылов В. В. Информационное копирование преступления / В.В. Крылов – М., 1997. С. 67.

имеет место указание на строгую связь с местонахождением, то есть туда осуществляется копирование информации: «создание идентичной копии в электронном носителе информации».[100] А.И. Халлиулин также включает в неправомерное копирование не только создание копии самой компьютерной информации, но и ее атрибутов, таких как размер файла, наименование, дата создания, сведения об авторе и иные реквизиты.[101] Отсутствие последних не позволяет сделать вывод о появлении копии в истинном смысле этого слова.

Анализа судебной практики показывает, что в большинстве случаев копированием признается перенос информации на флеш-карты и иные технические устройства, в том числе и на то же устройство, где хранилась информация, то есть копирование в узком смысле.

Правильное понимание сущности копирования тесно связано с установлением объекта рассматриваемого преступления. Под непосредственным объектом неправомерного доступа к компьютерной информации понимаются общественные отношения, которые обеспечивают право законного владельца компьютерной информации на ее безопасное создание, хранение и передачу.[102] Такая совокупность общественных отношений, которые возникают по поводу безопасности компьютерной информации.[103] Обязательным признаком копирования информации является то обстоятельство, что при наступлении данного последствия не происходит внесения каких-либо изменений в оригинал, то есть он остается в неизменном виде. В противном случае можно говорить о наступлении иных последствий, предусмотренных ст. 272 УК РФ: уничтожении, блокировании и модификации. В указанных случаях вред причиняется самой информации непосредственно, существенно затрудняется или делается невозможным ее использование в дальнейшем обладателем информации. При копировании этого не происходит,

---

[100] Абов А. И. Преступления в сфере компьютерной информации. / А.И. Абов – Москва : 2002. С. 13.

[101] Халлиулин А. И. Неправомерное копирование как последствие преступлений в сфере компьютерной информации [Электронный ресурс] / А. И. Халлиулин // Российский следователь. 2015. № 8. – Режим доступа: http://www.consultant.ru.

[102] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[103] Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации : дисс …. канд. юр. наук. : 12.00.08 / Малышенко Дмитрий Геннадьевич. – М., 2009. С. 56.

так как нарушается ее конфиденциальность, что свойственно самому деянию ст. 272 УК РФ – неправомерному доступу к компьютерной информации.[104] Копирование компьютерной информации не несет в себе такой общественной опасности, которая была бы равноценна модификации, блокированию или уничтожению, то есть иным альтернативным признакам данного преступления. Представляется, что реальную общественную опасность, причиняющую вред объекту, составляет дальнейшее противоправное использование, но не копирование как таковое.

Сказанное подтверждается реальной правовой действительностью. Согласно приведенному исследованию статистики применения нормы о неправомерном доступе к компьютерной информации, повлекшему ее копирование, в большинстве случаев суды квалифицируют данное деяние по правилам идеальной совокупности со статьями, предусматривающими ответственность за посягательство на информацию граждан и организаций, доступ к которой ограничен. В российском уголовном законодательстве предусмотрен ряд статей, связанных с посягательствами на информацию граждан, доступ к которой ограничен: ст. 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений); ст. 146 УК РФ (Нарушение авторских и смежных прав); ст. 147 УК РФ (Нарушение изобретательских и патентных прав); ст. 183 УК РФ (Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну); ст. 283.1 (Незаконное получение сведений, составляющих государственную тайну) и другие.

Соответственно реальное фактическое использование компьютерной информации (которое непосредственно причиняет вред названным общественным отношениям) выражается в совершении иных самостоятельных преступлений, посягающих на иные непосредственные объекты. В указанных

[104] Айсанов Р. М. Состав неправомерного доступа к компьютерной информации, в Российском, международном и зарубежном уголовном законодательстве . : автореф. дис. …. канд. юр. наук : 12.00.08 / Айсанов Руслан Мухамедович. – Москва, 2006. 31 с.

наиболее распространенных случаях копирование компьютерной информации фактически выступает способом совершения других преступлений, оно описывается такими признаками составов как: «собирание», «присвоение», «приобретение», «получение», «изъятие» и др. Тем не менее, закрепление в ст. 272 УК РФ самостоятельного последствия в виде копирования не охватывается данными составами и требует квалификации по совокупности преступлений.

Так, согласно Постановлению Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации или посредством создания, использования и распространения вредоносных компьютерных программ, требует дополнительной квалификации по статье 272, 273 или 274.1 УК РФ.[105]

Аналогичное по сути разъяснение дано в п. 3 постановления Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 «О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации)», установлено, что под собиранием сведений о частной жизни лица понимаются умышленные действия, состоящие в получении этих сведений любым способом, например путем личного наблюдения, прослушивания, опроса других лиц, в том числе с фиксированием информации аудио-, видео-, фотосредствами, копирования документированных сведений, а также путем похищения или иного их приобретения.[106]

---

[105] О судебной практике по делам о мошенничестве, присвоении и растрате. [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[106] О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации) [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

Таким образом, копирование компьютерной информации можно отнести к разновидности собирания сведений о частной жизни лица, что и образует идеальную совокупность указанных преступлений.

Можно привести примеры из судебной практики.

Так, согласно приговору № 1-250/2018 от 13 июня 2018 г., виновный, используя свое служебное положение, в отсутствие заявления владельца абонентского номера, осуществил вход в компьютерную программу, где составил заявку на предоставление детализации номера абонента, что является конфиденциальной информацией, содержащей тайну переговоров, и отправил ее на электронный однодневный почтовый ящик. Действия виновного были квалифицированы по ч. 3 ст. 272 УК РФ, то есть неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование, совершенный лицом с использованием своего служебного положения. А также по ч. 2 ст. 138 УК РФ, то есть нарушение тайны телефонных переговоров, совершенное лицом, с использованием своего служебного положения.[107]

Так, согласно приговору № 1-283/2018 от 6 июня 2018 г., виновный, реализуя свой преступный умысел на незаконное собирание сведений, составляющих коммерческую тайну, используя учетную запись, логин и пароль потерпевшего, со своего рабочего компьютера осуществил вход в систему, и, незаконно скопировал базу данных клиентов ПАО на свой сотовый телефон для использования в личных целях. Действия были квалифицированы по ч. 1 ст. 272 (неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование) и по ч. 1 ст. 183 (незаконное получение сведений, составляющих коммерческую тайну).[108]

Согласно приговору № 1-41/2018 от 4 июня 2018 г., виновный, не имея возможности оплачивать услугу провайдера по предоставлению широкополосного доступа в сеть Интернет, действуя из корыстной

[107] Приговор Кировского районного суда г.Астрахани от 13.06.2018 № 1-250/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[108] Приговор Канавинского районного суда г.Нижний Новгород от 06.06.2018 № 1-283/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

заинтересованности в виде безвозмездного незаконного пользования услугами, оплаченными законными абонентами провайдера, скопировал в память своего компьютерного оборудования текстовый файл, содержащий регистрационные данные – логины и пароли законных абонентов провайдера. Действия виновного были квалифицированы по ч. 2 ст. 272 УК РФ (неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование, совершенный из корыстной заинтересованности).[109]

Подобную сложившуюся практику вряд ли можно назвать приемлемой. По нашему мнению, она приводит к неправильной излишней квалификации одного деяния по двум статьям и как следствие к двойной ответственности за преступление, что противоречит принципу справедливости, предусмотренному ч. 2 ст. 6 УК РФ. Решение этой проблемы, по нашему мнению, видится в возможности исключения из диспозиции ст. 272 УК РФ такого признака как копирование компьютерной информации, поскольку оно само по себе не причиняет вред объекту преступления, предусмотренного ст. 272 УК РФ. В нем нет той общественной опасности, которая была бы равноценна другим перечисленным в ней последствиям. Таким образом, копирование компьютерной информации должно быть квалифицировано по соответствующим статьям Уголовного кодекса в зависимости от того, какая конфиденциальная информация была получена таким образом, и какие права обладателя этой информации нарушены.

По этому пути пошли многие развитые правовые системы в сфере установления ответственности за неправомерный доступ к компьютерной информации.

Так, например п. 303 а) УК ФРГ («Изменение данных») не предусматривает такое последствие как копирование.

Ответственность за неправомерное копирование конфиденциальных данных в ФРГ предусмотрена другими статьями в разделе 15 УК ФРГ, к

[109] Приговор Зареченского районного суда г.Тулы от 04.06.2018 № 1-41/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

примеру, п. 202 (Нарушение тайны переписки); п.206 (Нарушение тайны почтовой и телекоммуникационной тайны) и иные. [110]

Ответственность за нарушение авторских, смежных и патентных прав при неправомерном копировании в ФРГ регулируется специальными законами, например, законом «Об авторском праве и смежных правах». В определенных случаях данное преступление влечет за собой ответственность в виде лишения свободы. [111]

Уголовный кодекс КНР также не содержит признака копирования в аналогичном преступлении. Так ст. 286 УК КНР содержит лишь такие признаки объективной стороны неправомерного доступа к компьютерной информации как: сокращение (изъятие) текста, исправление, дополнение, создание помех, приведшее к невозможности нормального функционирования компьютерной информационной системы.[112] При этом следует отметить, что указанные признаки характеризуют не последствия неправомерного доступа, а формы самого преступного деяния. Состав имеет конструкцию материального, обязательным признаком преступления является причинение существенного вреда в результате совершения указанных действий. Подобная правовая конструкция видится более правильной как с точки зрения отражения в ней общественной опасности преступления, так и правил законодательной техники.

В качестве возможного варианта нами предлагается также включить в КоАП состав правонарушения, предусматривающего ответственность за неправомерный доступ к компьютерной информации без указания наступления общественно-опасных последствий. Незаконное копирование следовало бы рассматривать как типичное последствие указанного правонарушения, не обладающего общественной опасностью. А в случае неправомерного дальнейшего использования информации, следует квалифицировать по

---

[110] Уголовный кодекс ФРГ [Электронный ресурс] // Российский правовой портал: библиотека Пашкова. – Режим доступа: http://www.constitutions.ru.

[111] Об авторском праве и смежных правах [Электронный ресурс] : закон ФРГ// Адвокатская канцелярия. – Режим доступа: http://www.advokat-engelmann.de

[112] Уголовный кодекс КНР [Электронный ресурс] // Посольство Китайской Народной Республики в Российской Федерации. – Режим доступа: http://ru.china-embassy.org

соответствующим статьям УК РФ.

Таким образом, к последствиям данного преступления, предусмотренного ст. 272 УК РФ следует относить уничтожение (в случае если информация не подлежит восстановлению), блокирование и модификацию компьютерной информации.

Следует отметить, что наступление нескольких последствий, при совершении неправомерного доступа не образуют совокупности преступлений.

Так, приговором Ленинского суда г.Тамбова № 1-60/2019 от 21 марта 2019 г. установлено, что виновный, находясь на рабочем месте имел целью осуществление неправомерного доступа к компьютерной информации, а именно доступа к операционной системе, которая содержалась в памяти игровой приставки. Так, законным правообладателем оригинального программного обеспечения игровой приставки является организация. Виновный, используя свои специальные познания, с помощью специализированного программного обеспечения, которое предназначено для изменения содержимого, находящегося во внутренней памяти устройства, осуществил неправомерный доступ к оригинальному программному обеспечению игровой приставки. Далее, виновный внес такие изменения, которые не были разрешены производителем приставки, в программное обеспечение, таким образом, осуществил модификацию. Соответственно, преодолев программно-технические средства защиты информации, использованные производителем для защиты от применения нелицензионных программ. Данные действия привели к возможности воспроизведения на игровой приставке нелицензионный программный продукт.

Использование вышеуказанной нелицензионной компьютерной программы привело к уничтожению оригинального программного обеспечения, Так на игровой приставке оно было заменено на нелицензированную копию.

Так, лицо осуществило неправомерный доступ к компьютерной информации, повлекший ее уничтожение и модификацию, то есть преступление, предусмотренное ч.1 ст. 272 УК РФ. [113]

Таким образом, суды правильно квалифицируют деяние при наступлении нескольких альтернативных последствий как одно преступление.

Существует позиция ученых, согласно которой состав преступления, предусмотренного статьей 272 УК РФ необходимо преобразовать в формальный, и соответственно, наступившие последствия (копирование, блокирование, модификация и уничтожение компьютерной информации) необходимо отразить в качестве признака квалифицированного состава преступления.

Так, А.Е. Шарков в своих исследованиях приходит к выводу о необходимости исключения из диспозиции ч. 1 ст. 272 УК РФ обязательного признака в виде наступления последствий. Такие последствия, по его мнению, должны влечь за собой более строгую ответственность.[114]

По нашему мнению, такой подход нецелесообразен, поскольку ответственности за неправомерный доступ Уголовный кодекс не предусматривает. Неправомерный доступ не является также правонарушением. Сам по себе неправомерный доступ к компьютерной информации без наступления последствий не причиняет вреда объекту посягательства.

Причинную связь необходимо определить как такое отношение между явлениями, при котором одно или несколько явлений – причина порождает другое явление – следствие.[115]

Так, для привлечения лица к ответственности за неправомерный доступ к компьютерной информации необходимо, чтобы деяние находилось в причинной связи между действиями виновного лица и вредными последствиями, указанными в диспозиции ст. 272 УК РФ.

---

[113] Приговор Ленинского суда г.Тамбова № 1-60/2019 от 21 марта 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.
[114] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.
[115] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 124.

Состав преступления, предусмотренного ст. 272 УК РФ является материальным, и преступление считается оконченным с момента наступления одного из последствий, предусмотренного статьей.

Деяние следует квалифицировать как покушение или приготовление к преступлению, в случае если, лицо имело умысел на уничтожение, блокирование, модификацию, копирование информации, однако последствия не наступили.

Приготовлением к преступлению будут являться такие действия как получение логинов и паролей, планирование технической стороны совершения преступления, подыскание специализированных программ для доступа, с целью копирования, блокирования, модификации или уничтожения информации.

По мнению А.Ю. Решетникова, Е.А. Русскевич, в случае, если лицо, которое совершило неправомерный доступ к охраняемой законом компьютерной информации и затем попыталось ее уничтожить, модифицировать, блокировать, копировать, но преступная цель оказалась не реализована по не зависящим от лица обстоятельствам, такие действия следует оценивать как покушение на уничтожение, модификацию, блокирование или копирование охраняемой законом компьютерной информации по ч. 3 ст. 30 и ч. 1 ст. 272 УК РФ. Так, например, действия могут быть не доведены до конца вследствие задержания, иных причин.[116]

Так, согласно приговору Ленинского районного суда г. Владимира № 1-211/2018 от 27 июля 2018 г. по делу № 1-211/2018, виновный совершил покушение на неправомерный доступ к охраняемой законом компьютерной информации, повлекшее копирование компьютерной информации, из корыстной заинтересованности. Так, у лица возник преступный умысел и корыстная цель, направленные на незаконный удаленный доступ к информационным ресурсам органов государственной власти с целью копирования компьютерной информации, расположенной на данных ресурсах.

[116] Решетников А.Ю. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации [Электронный ресурс] / А.Ю. Решетников, Е.А. Русскевич // Уголовное право. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

Так это информация содержала сведения об адресах почтовых ящиков пользователей ресурсом, а также паролях к данным почтовым ящикам. В связи с этим виновный получил возможность в дальнейшем использования данных пользователей в целях получения доступа в электронной платежной системе к их счетам, и последующего перевода денежных средств со счетов потерпевших на свой счет в данной платежной системе. По не зависящим обстоятельствам, действия виновного не доведены до желаемого преступного результата. Так виновный не смог преодолеть систему защиты, установленную на официальном сайте администрации региона.[117]

Согласно приговору Белгородского районного суда Белгородской области от 16 сентября 2010 г. по делу № 1-43/2010, лицо было осуждено по ч. 3 ст. 30, ч. 1 ст. 272 УК РФ. Так виновный совершил покушение на неправомерный доступ к охраняемой законом компьютерной информации, влекущий ее модификацию. В соответствии с вынесенным приговором виновный имел целью неправомерный доступ к охраняемой законом информации для ее модификации, руководствуясь корыстными побуждениями. В данном случае, проводя ОРМ – «проверочная закупка», оперативный сотрудник выступил в роли заказчика и сделал заказ виновному на сумму 200 рублей. Суть заказа заключалась в изменении IMEI мобильного телефона, то есть международного идентификатора, который изменению не подлежит в связи с тем, что является уникальным номером, который присваивается мобильному устройству. Данный номер позволяет мобильному оператору и иным служащим обнаружить телефон, идентифицировать его в случае хищения, потери. В целях изменения IMEI номера, виновный, осуществляя умысел, использовал специальную программу, установленную на специальном устройстве, к которому и подключил переданный ему оперативным сотрудником мобильный телефон. Продолжая свои преступные действия, лицо получило доступ к охраняемой законом компьютерной информации – IMEI-номеру, используя программу на

[117] Приговор Ленинского районного суда г. Владимира № 1-211/2018 от 27 июля 2018 г. по делу № 1-211/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

специальном устройстве, к которому подключен мобильный телефон, и соответственно получил возможность воздействия на эту информации. Таким образом, лицо произвело модификацию компьютерной информации, изменив идентификационный номер мобильного телефона с помощью специальной программы. Вынося решения, суд учитывал то, что данные действия проходили в рамках ОРМ, то есть осуществлялся контроль правоохранительными органами, в связи с чем причинение вреда общественным отношениям в информационной сфере не наступил, однако квалифицировал действия по статье 272 УК РФ, как неправомерный доступ к компьютерной информации, повлекший ее модификацию.[118]

Однако в том случае, когда лицо по независящим обстоятельствам не смогло скопировать, уничтожить, модифицировать, блокировать желаемый определенный объем компьютерной информации, содеянное виновным так или иначе образует оконченное преступление. Несмотря на тот факт, что умысел виновного не был реализован до конца, это свидетельствует лишь о фактической незавершенности деяния, но в юридическом смысле оно было окончено с момента копирования, уничтожения или первого файла, блокирования или модификации части информации.[119]

Также в науке существуют факультативные признаки субъективной стороны, такие как место, способ, время, которые имеют значение для квалификации деяния в случае, если в статье закона они прямо закреплены. Для квалификации деяния по ст. 272 УК РФ такие признаки значения не имеют.

Так, под способом совершения преступления понимается порядок, метод, последовательность движений и приемов, применяемых лицом в про-цессе реализации преступных намерений.[120]

---

[118] Приговор Белгородского районного суда Белгородской области от 16 сентября 2010 г. по делу № 1-43/2010 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[119] Решетников А.Ю. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации [Электронный ресурс] / А.Ю. Решетников, Е.А. Русскевич // Уголовное право. – 2018. – № 2. Режим доступа: http://www.consultant.ru.

[120] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 137.

По мнению В.Г. Степанова-Егиянца существуют различные способы осуществления неправомерного доступа, используя различные приемы обмана системы защиты информации, а также использование чужого пользовательского имени, варианты подбора паролей, изменение адреса электронно-технического устройства, нахождение и использование пробелов и минусов в программах, которые можно использовать для обхода системы.[121]

А.Г. Волеводз под способами понимает «нейтрализацию установленных средств защиты при помощи специализированных технических устройств и программ, вход в систему от имени законного пользователя при помощи чужих паролей, совершения иных действий, хищение материальных носителей информации, если это повлекло копирование, блокирование, модификацию либо уничтожение компьютерной информации и при условии применения к информации мер по ее охране».[122]

Так, говоря о способе, можно сделать вывод, что большинство преступлений совершаются путем перехвата информации с помощью компьютерной и иной техники, используя различные программы, пароли и иные средства.

Под временем совершения преступления понимается конкретный период, отрезок времени, выраженный через какое-либо событие или временной промежуток.[123]

Согласно ч. 2 ст. 9 УК РФ, временем совершения преступления признается время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий.

Таким образом, временем совершения преступления, предусмотренного ст. 272 УК РФ признается время совершения неправомерного доступа к компьютерной информации, вне зависимости от времени наступления общественно-опасных последствий.

---

[121] Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[122] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Электронный ресурс] : монография / А. Г. Волеводз – Москва : Юрлитинформ, 2011. – Режим доступа: http:// www.mgimo.ru.

[123] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 136.

Под местом совершения преступления понимается такая территория, территориальное пространство, на которой было совершено преступление.[124]

Компьютерные преступления имеют трансграничный характер. Деяние может быть совершено на территории одного государства, однако последствия могут распространяться и на другие страны.

Так, согласно ч. 2 ст. 9 УК РФ, временем совершения преступления признается время совершения общественно опасного действия (бездействия) независимо от времени наступления последствий. Следовательно, местом признается место совершения общественно-опасного деяния.

Таким образом, местом совершения преступления, предусмотренного ст. 272 УК РФ будет являться место, где совершен неправомерный доступ к компьютерной информации, вне зависимости от того где наступили общественно-опасные последствия.

Таким образом, место, способ, время совершения преступления не являются признаками объективной стороны преступления, предусмотренного ст. 272 УК РФ, на квалификацию не влияют.

1.3 Субъект неправомерного доступа к компьютерной информации

В международном уголовном праве под субъектом компьютерных преступлений понимаются как физические, так и юридические лица. В соответствии с Конвенцией Совета Европы о преступности в сфере компьютерной информации ETS № 185 от 23 ноября 2001 г. субъектом компьютерных преступлений могут быть физические и юридические лица. Согласно ст. 12 Конвенции, «каждая Сторона принимает законодательные и иные меры, необходимые для обеспечения возможности привлечения юридических лиц к ответственности за уголовное преступление, предусмотренное в соответствии с настоящей Конвенцией, которое совершается в их пользу любым физическим лицом, действующим

[124] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. С. 136.

самостоятельно или как часть одного из органов соответствующего юридического лица и занимающим ведущее положение в нем».[125]

На данный момент в Российской Федерации, только физические лица могут подлежать уголовной ответственности.

В науке под субъектом преступления принято понимать вменяемое физическое лицо, достигшее возраста уголовной ответственности, который предусмотрен Уголовным кодексом Российской Федерации.[126]

Согласно диспозиции ст. 272 УК РФ существуют два вида субъектов неправомерного доступа к компьютерной информации: общий и специальный.

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

В науке существует мнение относительно возраста, с которого наступает ответственность за данное преступление. Так преступления в сфере компьютерной информации часто совершаются лицами, не достигшими 16 лет. Несовершеннолетние, не достигшие шестнадцати лет, зачастую обладают навыками работы с компьютером, по сравнению с людьми старшего возраста. В том числе лица, не достигшие шестнадцати лет, в полной мере могут осознавать общественную опасность совершаемых ими действий, а также предвидеть наступление последствий (разной степени тяжести) преступления, предусмотренного ст. 272 УК РФ.

По мнению В.Г. Степанова-Егиянца, необходимо снизить возраст наступления уголовной ответственности за совершение преступления, предусмотренного ст. 272 УК РФ, до 14 лет. [127]

Также, по мнению А.Ж. Кабановой, минимальный возраст уголовной

---

[125] Европейская конвенция по киберпреступлениям от 21.11.2001 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[126]Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – М.: Проспект, 2011. С. 138.

[127]Степанов-Егиянц В. Г. Характеристика субъекта неправомерного доступа к компьютерной информации по Уголовному кодексу РФ [Электронный ресурс] / В. Г. Степанов-Егиянц // Законодательство. – 2014. – № 7. – Режим доступа: https://base.garant.ru.

ответственности за преступление, предусмотренное ст. 272 УК РФ, должен быть снижен в силу «большой доступности технических средств хранения, обработки и передачи информации большинству населения».[128]

Р.М. Айсанов в своей работе утверждает, что снижение возраста уголовной ответственности за неправомерный доступ к компьютерной информации до 14 лет «предупредит вовлечение с целью использования под предлогом безответственности подростков в организованные криминальные структуры и ограничит мотивацию подростковой шалости».[129]

Существует иная позиция ученых. Так, И.А. Сало, В.С. Карпов выступают против снижения ответственности за данное преступления. В обоснование своей позиции они приводят следующие аргументы: противоречие принципу гуманности, принципу уголовной репрессии, сниженное психическое отношение к собственным действиям по сравнению с отношением лиц, достигших 16 лет.[130]

По нашему мнению, снижать возраст уголовной ответственности за данное преступление нецелесообразно, поскольку для совершения данного преступления необходимы определенные навыки и знания, а также осознание причинения вреда своими действиями. В данном случае, хоть и происходит внедрение техники в жизнь несовершеннолетних, однако лица до 16 лет не всегда понимают и осознают свои действия в данной сфере и возможность причинения вреда посредством технических устройств.

Специальным субъектом неправомерного доступа к охраняемой законом компьютерной информации является физическое вменяемое лицо, достигшее 16-летнего возраста, обладающее на момент совершения преступления дополнительными признаками, присущими ему на момент совершения

---

[128]Кабанова А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты). : автореф. дис. ... канд. юрид. наук. 12.00.08 / Кабанова Анна Жунусовна. – Ростов-на-Дону, 2004. – 28 с.

[129]Айсанов Р. М. Состав неправомерного доступа к компьютерной информации, в Российском, международном и зарубежном уголовном законодательстве . : автореф. дис. …. канд. юр. наук : 12.00.08 / Айсанов Руслан Мухамедович. – Москва, 2006. – 31 с.

[130] Степанов-Егиянц В. Г. Характеристика субъекта неправомерного доступа к компьютерной информации по Уголовному кодексу РФ [Электронный ресурс] / В. Г. Степанов-Егиянц // Законодательство. – 2014. – № 7. – Режим доступа: https://base.garant.ru.

общественно опасного деяния, и способное нести уголовную ответственность за преступление.[131]

Специальным субъектом считается лицо, совершившее неправомерный доступ к компьютерной информации с использованием своего служебного положения. Так, часть 3 ст. 272 УК РФ предусматривает совершение преступления специальным субъектом – лицом с использованием своего служебного положения. Анализ данного признака будет рассмотрен нами далее в третьей главе.

1.4 Субъективная сторона неправомерного доступа к компьютерной информации

Субъективной стороной преступления называют психическую деятельность лица, непосредственно связанную с совершением преступления.

Умысел и неосторожность – формы вины, составляющие субъективную сторону преступлений. Необходимо указать, что обязательными признаками субъективной стороны являются данные формы вины – умысел и неосторожность. При этом мотивы и цели остаются факультативными признаками.[132]

Согласно Европейской конвенции по киберпреступлениям от 21.11.2001, незаконный доступ может осуществляться только умышленно. Так в ст. 2 сказано, что каждая из Сторон должна принять такие меры законодательного и иного характера, чтобы установить в своем внутреннем законодательстве в качестве уголовно наказуемого деяния противоправный умышленный доступ к компьютерной системе в целом или любой ее части.[133]

Согласно «Методическим рекомендациям по осуществлению

---

[131] Степанов-Егиянц В. Г. Характеристика субъекта неправомерного доступа к компьютерной информации по Уголовному кодексу РФ [Электронный ресурс] / В. Г. Степанов-Егиянц // Законодательство. – 2014. – № 7. – Режим доступа: https://base.garant.ru.

[132] Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – М.: Проспект, 2011. С. 138.

[133] Европейская конвенция по киберпреступлениям от 21.11.2001 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», субъективная сторона рассматриваемого преступления характеризуется виной в форме прямого или косвенного умысла или неосторожности.[134]

В российской науке, существует точка зрения, в соответствии с которой неправомерный доступ к компьютерной информации может быть совершен только с прямым умыслом.[135]

Следующая группа исследователей, таких как Ю. Ляпунов, В. Максимов, Л.А. Сударева, придерживается позиции, согласно которой субъективная сторона неправомерного доступа к компьютерной информации характеризуется виной в форме прямого и косвенного умысла. Соответственно, лицо должно осознавать общественную опасность своего деяния, предвидеть возможность или неизбежность наступления общественно опасных последствий и желать их наступления, либо допускать их, или относиться к ним безразлично.[136]

Некоторые ученые считают, что неправомерный доступ к компьютерной информации может быть совершен как умышленно, так и по неосторожности. Такие ученые как С А. Пашин, С.Н. Золотухин и А.З. Хун указывают, что форма вины в виде неосторожности наличествует тогда, когда лицо совершает ошибку при оценке своего доступа к компьютерной информации с точки зрения правомерности, и наступления указанных в законе последствий.[137]

С точки зрения В.С. Карпова вид последствия преступления определяет форму вины. Автор, обосновывая свой вывод, утверждает, что в случае, когда деяние преступника направлено на достижение его преступных целей, то есть тех результатов, которые он желает, имеет место прямой умысел. В данном

---

[134]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[135]Степанов-Егиянц В. Г. Субъективная сторона компьютерных преступлений [Электронный ресурс] / В. Г. Степанов-Егиянц // Бизнес в законе. Экономико-юридический журнал. – 2013. – № 2. – Режим доступа: http://www.cyberleninka.ru.

[136]Там же.

[137]Степанов-Егиянц В. Г. Субъективная сторона компьютерных преступлений [Электронный ресурс] / В. Г. Степанов-Егиянц // Бизнес в законе. Экономико-юридический журнал. – 2013. – № 2. – Режим доступа: http://www.cyberleninka.ru.

случае с прямым умыслом может совершаться копирование. Говоря об иных последствиях, указанных в законе, то есть блокирование, модификация, уничтожение информации совершаются с прямым или косвенным умыслом либо по неосторожности. При этом необходимо учитывать обстоятельства дела, направленность умысла, обстоятельства совершения деяния.[138]

А.Г. Волеводз считает, что субъективная сторона данного преступления выражается в том, что лицо совершает преступление с прямым умыслом. Последствия могут наступать в результате наличия косвенного умысла и по неосторожности.[139]

Согласно мнению В.Г. Степанова-Егиянца признак неправомерности, указанный в статье Уголовного закона подразумевает совершение преступления только умышленно, то есть с прямым или косвенным умыслом. Так, виновный осознает, что совершает неправомерный, ограниченный доступ к охраняемой законом компьютерной информации.[140] Согласиться с такой позицией не представляется возможным, поскольку признак неправомерности отражает исключительно объективную сторону преступления.

Исходя из анализа судебной практики, связанной с привлечением к ответственности по статье 272 УК РФ, можно сделать вывод о том, что суды при разбирательстве уголовных дел устанавливают умысел на совершение неправомерного доступа к охраняемой законом компьютерной информации.

Так, согласно Приговору Егорьевского городского суда Московской области № 1-220/2019 от 15 апреля 2019 г., виновный, реализуя умысел, совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование, из корыстной заинтересованности, которая выразилась в желании получить денежное вознаграждение за свои деяния в размере 3000 рублей. Суд квалифицировал деяние по ч. 2 ст. 272 УК

---

[138]Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации : дис….канд. юридических наук : 12.00.08 / Карпов Виктор Сергеевич. – Красноярск, 2002. – 134 с.
[139]Волеводз А. Г. Указ. соч. – Режим доступа: http:// www.mgimo.ru.
[140]Степанов-Егиянц В. Г. Субъективная сторона компьютерных преступлений [Электронный ресурс] / В. Г. Степанов-Егиянц // Бизнес в законе. Экономико-юридический журнал. – 2013. – № 2. Режим доступа: – http://www.cyberleninka.ru.

РФ, то есть неправомерный доступ к компьютерной информации, повлекший ее копирование, совершенный из корыстной заинтересованности.[141]

Приговором Октябрьского районного суда г. Ростова-на-Дону № 1-306/2019 от 22 апреля 2019 г. установлено, что виновный, имея преступный умысел, осуществил неправомерный доступ к охраняемой законом компьютерной информации, а именно в компьютерную программу, которая используется сотрудниками компании. Продолжая реализовывать свой преступный умысел, виновный передал через сеть Интернет скопированный им код абонентского номера. Таким образом, лицо, совершило преступление, предусмотренное ч. 2 ст. 272 УК РФ, то есть неправомерный доступ к компьютерной информации, повлекший ее блокирование, совершенный из корыстной заинтересованности.[142]

Согласно Приговору Энгельского районного суда Саратовской области № 1-1-203/2019 1-203/2019 от 21 марта 2019 г., виновный, реализуя свой преступный умысел, используя свое служебное положение, умышленно осуществил неправомерный доступ к охраняемой компьютерной информации, а также внес сведения, в программное обеспечение. Суд квалифицировал деяние по ч. 3 ст. 272 УК РФ, то есть как неправомерный доступ к компьютерной информации, повлекший ее модификацию, совершенный лицом с использованием своего служебного положения.[143]

Так, форма вины деяния не отграничивается судами от формы вины наступивших последствий, в связи с чем, суды устанавливают в деянии только умысел на совершение доступа к компьютерной информации, а также автоматически и умышленную форму вины в отношении наступивших последствий.

---

[141] Приговор Егорьевского городского суда Московской области от 15.04.2019 № 1-220/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[142] Приговор Октябрьского районного суда г. Ростова-на-Дону от 22.04.2019 № 1-306/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[143] Приговор Энгельского районного суда саратовской области от 21.03.2019 № 1-203/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

По нашему мнению, в ст. 272 УК РФ форма вины может выражаться в виде умысла, прямого и косвенного, а также в виде неосторожности. Однако, поскольку состав преступления является материальным, остается нерешенным вопрос о форме вины в отношении наступивших последствий.

Одним из вариантов решения данной проблемы является предложение об исключении из состава преступления деяния в виде неправомерного доступа. Таким образом, деянием будет признаваться неправомерное блокирование, модификация, уничтожение компьютерной информации. В данном случае состав будет являться формальным, а форма вины будет выражаться исключительно в виде прямого умысла, что свойственно сущности таких деяний как преступных.

Мотивы и цели неправомерного доступа к компьютерной информации не являются обязательным признаком состава преступления, предусмотренного ч. 1 ст. 272 УК РФ (так ч. 2 ст. 272 УК РФ, предусматривает ответственность за деяние, совершенное из корыстной заинтересованности), но их установление влияет на установление причин совершения преступления, а, следовательно, и назначение наказания.

Таким образом, неправомерный доступ к компьютерной информации это умышленное преступление, совершаемое как умыслом, а также по неосторожности, субъектом которого является вменяемое физическое лицо, достигшее возраста 16 лет, не имеющее права доступа к компьютерной информации.

2 Анализ квалифицирующих признаков преступления, предусмотренного ст. 272 УК РФ

Уголовный закон Российской Федерации не содержит понятия «квалифицирующий признак», однако в теории уголовного права данный термин широко используется.

Квалифицирующие признаки – это признаки состава преступления, отягчающие вину и в силу этого влияющие на квалификацию преступления, влекущие установление иной санкции.[144]

В связи с тем, что различные деяния несут в себе различную общественную опасность, в статьях закона предусмотрены квалифицирующие и особо квалифицирующие признаки.

Объективная сторона преступлений, предусмотренных ч. 2, 3, 4 ст. 272 УК РФ включает в себя деяние – «неправомерный доступ» к компьютерной информации, общественно-опасные последствия – уничтожение, блокирование, копирование, модификация компьютерной информации.

Часть 2 ст. 272 УК РФ предусматривает ответственность за неправомерный доступ к компьютерной информации, если это деяние причинило крупный ущерб, либо было совершено из корыстной заинтересованности.

Понятие «крупный ущерб» применяется для обозначения количественной характеристики последствий преступления.

Согласно примечанию 2 к ст. 272 УК РФ, крупным ущербом в статьях главы 28 признается ущерб, сумма которого превышает один миллион рублей. Данный признак был введен в ч. 2 ст. 272 УК РФ Федеральным законом от 7 декабря 2011 г. № 420-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации».

---

[144]Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В. Г. Степанов-Егиянц – Москва : Статут, 2016. – Режим доступа: http://www.consultant.ru.

Преступление, предусмотренное ч. 2 ст. 272 УК РФ, считается оконченным с момента причинения крупного ущерба. При отсутствии последствия в виде крупного ущерба преступное деяние следует квалифицировать по ч. 1 ст. 272 УК РФ. В случае если умысел лица был направлен на причинение крупного ущерба, содеянное следует квалифицировать по ч. 3 ст. 30 ч. 2 ст. 272 УК РФ, как покушение на неправомерный доступ к компьютерной информации, повлекший копирование, модификацию, блокирование либо уничтожение компьютерной информации, причинивший крупный ущерб.

Приговором Егорьевского городского суда Московской области № 1-377/2019 от 30 июля 2019 г. по делу № 1-377/2019 лицо признано виновным в совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ, то есть в совершении неправомерного доступа к компьютерной информации, повлекшего ее копирование, причинившего крупный ущерб, совершенного из корыстной заинтересованности.

Так, виновный путем копирования с цифрового носителя, в памяти которого имелось программное обеспечение, правообладателем которого является ФИО, установил в память жесткого магнитного диска системного блока покупателя программное обеспечение, являющееся охраняемой законом компьютерной информацией, с признаками контрафактности, а именно: один экземпляр программного обеспечения стоимостью 26000 евро, что, согласно курсу валют Центрального банка Российской Федерации, составляет 1874293 рублей 20 копеек. Виновный получил за свои незаконные действия от покупателя денежное вознаграждение в размере 1000 рублей.

Таким образом, виновный причинил крупный ущерб владельцу программного обеспечения, в размере 1874293 рублей 20 копеек.[145]

Приговором Кировского районного суда г. Хабаровска (Хабаровский край) № 1-3/2017 1-45/2016 от 23 марта 2017 г. по делу № 1-3/2017 лицо

[145] Приговор Егорьевского городского суда Московской области № 1-377/2019 от 30 июля 2019 г. по делу № 1-377/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

признано виновным в совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ, то есть в совершении неправомерного доступа к охраняемой законом компьютерной информации, повлекшего уничтожение компьютерной информации и причинение крупного ущерба.

В соответствии с установленными обстоятельствами, виновный, имея умысел на совершение преступления, а именно на уничтожение компьютерной информации, принадлежащей организации и хранящейся на ее сервере путем неправомерного доступа к ней. Указанные действия лица виновного привели к безвозвратному уничтожению охраняемой законом компьютерной информации. Среди сведений были уничтожены резервные копии баз данных, базы данных программистов организации, почтовый сервер, а также проекты компаний. Уничтожение этих сведений выразилось в причинении ущерба в виде затрат в размере 897 944 рубля на оплату работы в выходные и праздничные дня сотрудникам, оплату вынужденного простоя в размере 388 181 рубль, оплата вынужденных командировок сотрудников для проведения ревизии в размере 182 938 рублей.

Таким образом, лицо причинило организации крупный ущерб в размере 1 469 062 руб.[146]

При наличии у лица корыстной заинтересованности, преступное деяние также необходимо квалифицировать по ч. 2 ст. 272 УК РФ.

Закон не дает определения понятия «корыстная заинтересованность». Исходя из понимания данного термина в русском языке «корысть» считается стремлением лица получить материальную выгоду различными способами.[147]

В науке выделяется определение корыстной заинтересованности как стремление лица получить материальную выгоду или избавиться от затрат. Также представляет собой стремление лица путем совершения указанных в ч. 1 ст. 272 УК РФ действий получить для себя или других лиц выгоду

[146] Приговор Кировского районного суда г. Хабаровска (Хабаровский край) № 1-3/2017 1-45/2016 от 23 марта 2017 г. по делу № 1-3/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.
[147]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

имущественного характера, не связанную с незаконным безвозмездным обращением имущества в свою пользу или в пользу других лиц.[148]

В Постановлении Пленума Верховного Суда РФ от 16 октября 2009 г. № 19 «О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий» корыстная заинтересованность определяется, как стремление путем совершения неправомерных действий получить для себя или других лиц выгоду имущественного характера либо избавиться от материальных затрат.[149]

Приговором Мариинско-Посадский районный суд Чувашской республики № 1-54/2019 от 26 июля 2019 г. по делу № 1-54/2019 установлено, что лицо совершило неправомерный доступ к охраняемой законом компьютерной информации, что повлекло блокирование и модификацию, компьютерной информации, совершенное из корыстной заинтересованности. Данные действия были квалифицированы судом по ч. 2 ст. 272 УК РФ, а также по п. г) ч. 3 ст. 158 УК РФ. Так, виновный с помощью сотового телефона на системе «Андроид», подключившись посредством связи «WiFi» к открытой точке доступа к телекоммуникационной сети «Интернет», а также, используя ранее незаконно приобретенные логин и пароль, совершил неправомерный доступ к охраняемой законом компьютерной информации, и таким образом, блокировав и модифицировав компьютерную информацию, размещенную на странице потерпевшего в социальной сети «ВКонтакте».

После чего, виновный, из корыстных побуждений, с целью последующего хищения денежных средств, изменив идентификационные данные для доступа на данную электронную страницу и блокировав доступ к странице законного пользователя, с электронной страницы «АА» осуществил отправку сообщения с просьбой сообщить ему номер банковской карты, а также код для регистрации

[148]Оценочные признаки в Уголовном кодексе Российской Федерации: научное и судебное толкование [Электронный ресурс]: науч.-практ. пособие / под ред. А. В. Галаховой. – Москва : Норма. – 2014. – Режим доступа: http://www.consultant.ru.

[149]О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий [Электронный ресурс] Постановление Пленума Верховного Суда РФ от 16 октября 2009 г. № 19 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

в приложении «Сбербанк Онлайн» на электронный адрес электронной страницы «ВВ» социальной сети «ВКонтакте», принадлежащей потерпевшему, под предлогом перевода ему денежных средств в размере 5 000 рублей.

Получив указанное сообщение, потерпевший, находясь под воздействием обмана, сообщил виновному номер открытой на его имя банковской карты ПАО «Сбербанк», а также код для регистрации в приложении «Сбербанк Онлайн». После чего виновный из корыстных побуждений, тайно похитил с его банковского счета денежные средства в размере 4 700 рублей.[150]

Приговором Октябрьского районного суда г. Красноярска № 1-346/2019 от 8 июля 2019 г. по делу № 1-346/2019, лицо признано виновным в совершении преступления предусмотренного ч. 2 ст. 272 УК РФ, то есть неправомерный доступ к компьютерной информации, повлекший ее копирование, совершенный из корыстной заинтересованности. А также по ч. 2 ст. 159 УК РФ, как мошенничество с причинением гражданину значительного ущерба.

Так, виновный получил доступ к переписке электронного почтового ящика автомагазина «Доктор-Кар» где, увидев запрос от 12.01.2016 о намерении лица приобрести в автомагазине «Доктор-Кар» автоматическую коробку переключения передач (далее АКПП) модель U341F-03A на автомобиль «Toyota Voltz» («Тойота Вольтц»), решил похитить денежные средства, принадлежащие потерпевшему, путем предоставления последнему реквизитов имеющейся у него банковской карты для осуществления перевода денежных средств в счет оплаты товара, которого фактически у него не было.

Продолжая осуществлять свои преступные намерения, виновный направил с электронного почтового ящика от имени представителей автомагазина «Доктор-Кар» на электронный почтовый ящик потерпевшей письмо с предложением оплатить стоимость АКПП модель U341F-03A на указанный выше автомобиль в размере 12000 рублей

[150] Приговор Мариинско-Посадский районный суд Чувашской республики № 1-54/2019 от 26 июля 2019 г. по делу № 1-54/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

После поступления денежных средств на счет банковской карты, виновный снял денежные средства в сумме 12000 (двенадцать тысяч) рублей через терминал самообслуживания ПАО Сбербанк тем самым похитив их путем обмана.

Таким образом, в данном случае корыстная заинтересованность выразилась в стремлении получить материальную выгоду путем неправомерного доступа к охраняемой законом компьютерной информации.[151]

Часть 3 ст. 272 УК РФ предусматривает ответственность за деяния, предусмотренные частями первой или второй статьи 272 УК РФ, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

Согласно ч. 2 ст. 35 УК РФ, преступление признается совершенным группой лиц по предварительному сговору, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления.

Так, согласно Постановлению пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое», при квалификации действий группы лиц по предварительному сговору суду следует выяснять, имел ли место такой сговор соучастников до начала действий, состоялась ли договоренность о распределении ролей в целях осуществления преступного умысла, а также какие конкретно действия совершены каждым исполнителем и другими соучастниками преступления.

Приговором Центрального районного суда г. Читы № 1-54/2019 1-950/2018 от 20 февраля 2019 г. по делу № 1-54/2019, установлено, что виновные – ФИО1 и ФИО2 совершили неправомерный доступ к охраняемой законом компьютерной информации, который повлек копирование и модификацию компьютерной информации, совершенное группой лиц по предварительному сговору (ч. 3 ст. 272 УК РФ). Суд также квалифицировал деяния виновных по ч. 2 ст. 273, ч. 3 ст. 183, ч. 4 ст. 159.6 УК РФ.

[151] Приговор Октябрьского районного суда г. Красноярска № 1-346/2019 от 8 июля 2019 г. по делу № 1-346/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

Так, виновные вступили в предварительный сговор на хищение денежных средств у граждан, приобрели у неустановленного лица доступ к вредоносной программе – специализированной компьютерной программе, с помощью которой возможно получить доступ к информации. Данная программа предназначена для получения сведений о банковских счетах клиентов банков России, сведений о суммах денежных средств на счетах граждан, а также для удаленного управления мобильными банковскими приложениями. Так, указанные лица, согласовав преступные намерения, совместно получили доступ к охраняемой законом компьютерной информации – сведения о банковских счетах и иной информации, без разрешения законного владельца данной информации, то есть втайне от него. После чего, достоверно зная о сумме денежных средств потерпевшего, скопировали данную информацию с лицевого счета последнего, а также модифицировали информацию, которая выразилась в изменениях истории движения средств по счету, путем отправки сообщения на номер банка о списании денежных средств в размере девять тысяч рублей.[152]

Таким образом, заранее объединившись, лица совершали хищения денежных средств посредством неправомерного доступа к компьютерной информации, то есть совершали преступления группой лиц по предварительному сговору.

При квалификации возникают затруднения, в связи с тем, что преступление совершается группой лиц, однако непосредственно неправомерный доступ к компьютерной информации осуществляет один соучастник – непосредственный исполнитель. Так, По мнению В.Г. Степанова-Егиянца квалификацию необходимо осуществлять в зависимости от направленности умысла лиц. Если все соучастники имеют единый умысел, то действия каждого соучастника должны быть квалифицированы по ч. 3 ст. 272 УК РФ. Если совершается деяние, посягающее на другие общественные отношения, например отношения собственности, а неправомерный доступ

[152] Приговор Центрального районного суда г. Читы № 1-54/2019 1-950/2018 от 20 февраля 2019 г. по делу № 1-54/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

является способом совершения таких деяний, то по статье 272 УК РФ квалифицируются действия непосредственного исполнителя, то есть того лица, которое осуществило доступ к компьютерной информации.[153]

К. Н. Евдокимов имеет схожую точку зрения. По его мнению, неправомерный доступ к компьютерной информации сам по себе не часто встречается как самостоятельное преступление. Зачастую лица имеют иные преступные цели и такое деяние (неправомерный доступ) является способом для совершения других общественно опасных деяний. Поэтому действия виновных следует квалифицировать по совокупности совершенных преступлений.[154] По нашему мнению, данная позиция является верной, что подтверждается также судебной практикой.

Так, приговором от 05.08.2016 Кировоградского городского суда Свердловской области по делу № 1-105/2016 установлено, что согласно своей преступной роли виновный ФИО1, используя для совершения преступления вредоносные компьютерные программы, получил возможность неправомерного доступа к терминалу, принадлежащему организации, в связи с чем лицо смогло управлять движением безналичных денежных средств, доступ к которым осуществлялся с помощью указанного терминала. Кроме того, ФИО1 заказал две банковские карты, которые были зарегистрированы на иных лиц, имея намерения использовать заказанные банковские карты для перевода похищенных безналичных денежных средств ФИО2, который обладал информацией о пин-кодах от указанных карт.

Так, действия ФИО1 были квалифицированны по ч. 2 ст. 272 УК РФ, ч. 2 ст. 159.6, а действия ФИО2 были квалифицированы по ч. 2 ст. 159. 6, то есть за мошенничество в сфере компьютерной информации, совершенное группой лиц по предварительному сговору.

Таким образом, было установлено, что умысел обоих был направлен

---

[153]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.

[154]Евдокимов К. Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела [Электронный ресурс] / К. Н. Евдокимов – Российский следователь. – 2017. – № 4. – Режим доступа: http://www.consultant.ru.

именно на мошенничество, а неправомерный доступ к компьютерной информации был способом осуществления мошенничества в сфере компьютерной информации. Поэтому, так как непосредственно осуществлен неправомерный доступ к компьютерной информации одним лицом, то соответственно только его действия были квалифицированы по ст. 272 УК РФ.[155]

Согласно ч. 3 ст. 35 УК РФ, преступление признается совершенным организованной группой, если оно совершено устойчивой группой лиц, заранее объединившихся для совершения одного или нескольких преступлений.

Так, согласно Постановлению пленума Верховного Суда РФ от 27.12.2002 № 29 «О судебной практике по делам о краже, грабеже и разбое», в отличие от группы лиц, заранее договорившихся о совместном совершении преступления, организованная группа характеризуется, в частности, устойчивостью, наличием в ее составе организатора (руководителя) и заранее разработанного плана совместной преступной деятельности, распределением функций между членами группы при подготовке к совершению преступления и осуществлении преступного умысла. Об устойчивости организованной группы может свидетельствовать не только большой временной промежуток ее существования, неоднократность совершения преступлений членами группы, но и их техническая оснащенность, длительность подготовки даже одного преступления, а также иные обстоятельства (например, специальная подготовка участников организованной группы к проникновению в хранилище для изъятия денег (валюты) или других материальных ценностей).[156]

Так, приговором Якутского городского суда № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018 установлено, что лица совершили неправомерный доступ к компьютерной информации повлекший модификацию и копирование компьютерной информации, из корыстной заинтересованности,

---

[155]Приговор Кировоградского городского суда Свердловской области от 05.08.2016 по делу № 1-105/2016 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

[156]О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс] Постановлению пленума Верховного Суда РФ от 27.12.2002 № 29// Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

совершенный организованной группой. Действия виновных квалифицированы судом по ч. 3 ст. 272, ч. 2 ст. 273 и ч. 4 ст. 159.6 УК РФ.

Установлено, что виновные в неустановленном месте и при неустановленных обстоятельствах вступили между собой в преступный сговор, объединившись общим преступным умыслом, договорились о создании устойчивой организованной преступной группы. При этом, имея руководителя, объединившиеся единым преступным умыслом неустановленные лица разработали общий план преступной деятельности организованной группы, который предусматривал совместные координируемые и синхронизируемые, поэтапные и одновременные действия соучастников.

Так, лицо, действующее под псевдонимом «Директор» и другие лица, в том числе, обладающие специальными познаниями и навыками в сфере компьютерной информации, объединились из корыстной заинтересованности с целью систематических хищений денежных средств кредитно-финансовых учреждений. При помощи программ нейтрализации средств защиты компьютерной информации, и иного вмешательства в функционирование средств хранения, обработки и передачи компьютерной информации, а также информационно-телекоммуникационных сетей, осуществляли доступ к охраняемой законом компьютерной информации.

Таким образом, посредством получения неправомерного доступа к охраняемой законом компьютерной информации, хранящейся в локальных сетях, на серверах коммерческих банков и персональных компьютерах банковских сотрудников, осуществляли модификацию и копирование этой компьютерной информации и совершали систематические хищения денежных средств из кредитно-финансовых учреждений.[157]

Приговором от 10.10.2014 Перовского районного суда г. Москвы по делу № 1-975/2014 установлено, что лицо совершило неправомерный доступ к охраняемой законом компьютерной информации, и это деяние повлекло

[157] Приговор Якутского городского суда № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

модификацию компьютерной информации, совершенное организованной группой.

Для исполнения своих преступных намерений, действуя согласно разработанному плану, лицо совершило действия, направленные на организацию и функционирование организованной группы, которая была сформирована на этнической основе. Виновный, по национальности – узбек, проживая в РФ, являлся членом узбекской диаспоры в России. Он же решил собрать участников организованной группы по национальному признаку, а именно сограждан из Узбекистана, поскольку имел к ним повышенное доверие. Так, была создана организованная группа, основанная на общности интересов, национальности, мировоззрения, моральных качеств и принципов, которая в силу связей между участниками являлась устойчивой и имела иерархию. Далее, виновный разработал план преступных посягательств, нацеленный на нарушения общественных отношений, связанных с исполнением налоговых обязанностей и налоговой отчетностью, оборотом денежных средств, состоящий из последовательных действий различного характера, осуществляемых участниками организованной группы. Начав коммерческую деятельность по реализации товаров и оказанию услуг гражданам, виновные скрывали от ФНС РФ размер полученных доходов. Данные действия выполнялись при помощи использования специальной программы, которая после осуществления неправомерного доступа позволяла модифицировать информацию о денежных расчетах и операциях.

Таким образом, виновный, выступив лидером организованной группы, осуществлял руководство и организацию ее деятельности, путем распределения ролей между ее членами. Данные действия лица были квалифицированны по ч. 3 ст. 272 УК РФ.[158]

В настоящее время п. 3 ст. 272 УК РФ объединяет в себе оба признака, а именно совершение преступления группой лиц по предварительному сговору и

[158]Приговор Перовского районного суда города Москвы от 10.10.2014 по делу № 1-975/2014 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

организованной группой. По нашему мнению, совмещение в одном пункте статьи различных по общественной опасности обстоятельств является законодательным несовершенством. Так, в Уголовном кодексе такие признаки состава как совершение преступления группой лиц по предварительному сговору и организованной группой соотносятся в различных главах как квалифицирующий и особо квалифицирующий признак. Нами представляется возможным выделить данные признаки в разные пункты статьи и усилить ответственность за совершение неправомерного доступа к компьютерной информации, совершенного организованной группой, поскольку совершение деяния в составе организованной группы несет в себе большую общественную опасность, нежели совершение неправомерного доступа группой лиц по предварительному сговору.

Специальным субъектом преступления предусмотренного ч. 3 ст. 272 УК РФ является физическое вменяемое лицо, достигшее установленного законом возраста, которое обладает дополнительными признаками в момент совершения преступления. Таким дополнительным признаком является совершение деяния с использованием своего служебного положения.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», под использованием служебного положения, предусмотренного в диспозиции ч. 3 ст. 272 УК РФ, понимается использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ (в данном случае субъектом преступления не обязательно является должностное лицо), то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения (программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по

эксплуатации электронно-вычислительной техники и прочие).[159]

В науке нет единого мнения, что понимать под служебным положением.

Согласно первой точке зрения «использование служебного положения» означает, что лицо осуществляет неправомерный доступ незаконно, но в связи с выполняемой служебной деятельностью, то есть использует предоставленные ему на этой службе права.

Так, под специальным субъектом преступления, предусмотренного ч. 3 ст. 272 УК РФ, по признаку совершения преступления лицом с использованием своего служебного положения понимают должностных лиц, государственных служащих и служащих органов местного самоуправления, не являющихся должностными, лиц, выполняющих управленческие функции в коммерческой или иной организации. Другими словами, специальным субъектом признаются лица, перечисленные в примечаниях к статьям 201 и 285 УК РФ.

Так, согласно примечанию к ст. 201 УК РФ, выполняющим управленческие функции в коммерческой или иной организации, а также в некоммерческой организации, не являющейся государственным органом, органом местного самоуправления, государственным или муниципальным учреждением признается лицо, выполняющее функции единоличного исполнительного органа, члена совета директоров или иного коллегиального исполнительного органа, а также лицо, постоянно, временно либо по специальному полномочию выполняющее организационно-распорядительные или административно-хозяйственные функции в этих организациях.

Должностными лицами, в соответствии с примечанием к ст. 285, признаются лица, постоянно, временно или по специальному полномочию осуществляющие функции представителя власти либо выполняющие организационно-распорядительные, административно-хозяйственные функции в государственных органах, органах местного самоуправления,

[159]Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

государственных и муниципальных учреждениях, государственных корпорациях, государственных компаниях, государственных и муниципальных унитарных предприятиях, акционерных обществах, контрольный пакет акций которых принадлежит Российской Федерации, субъектам Российской Федерации или муниципальным образованиям, а также в Вооруженных Силах Российской Федерации, других войсках и воинских формированиях Российской Федерации.

Согласно второй точке зрения, лицо признается специальным субъектом не в связи с его положением по службе (должностное лицо, лицо, выполняющее управленческие функции в коммерческой и иной организации), а в связи с тем, что лицо, занимая определенное служебное положение имеет возможность доступа и соответственно может совершить преступление.[160]

В. Г Степанова-Егиянца в своей работе отражает те необходимые особенности, которые важны для квалификации преступления по ч. 3 ст. 272 УК РФ являются:

- наличие реального доступа к компьютерной информации. Таким образом, если у лица отсутствуют служебные обязанности, либо они прекращены, действия квалифицируются по ч. 1 ст. 272 УК РФ;

- лицо имеет особое право – преимущество для доступа к информации. Наоборот, если лицо, не имея преимущественного права, совершил преступление со служебного компьютера, то он не пользовался своим служебным положением, и, следовательно, деяние следует квалифицировать по ч. 1 ст. 272 УК РФ.[161]

По нашему мнению, субъектом данного преступления являются как должностные лица, лица, выполняющие управленческие функции в коммерческой или иной организации, так и лица, хоть и не являющиеся таковыми, но имеющие на законных основаниях, в силу трудового или гражданско-правового договора и должностной инструкции, возможность

[160]Степанов-Егиянц В. Г. Указ. соч. – Режим доступа: http://www.consultant.ru.
[161] Там же.

доступа к такой информации, и ее использования. Лицо, выполняющее трудовые функции в организации, в связи с этим, имея облегченный доступ к компьютерным программам и системам, но не имеющее право на осуществление доступа к охраняемой законом компьютерной информации, и осуществляющее доступ к такой информации, подлежит уголовной ответственности по ч. 1 ст. 272 УК РФ.

Так, приговором Ленинского районного суда г. Пензы № 1-145/2019 от 17 июля 2019 г. по делу № 1-145/2019, лицо признано виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, то есть неправомерного доступа к охраняемой законом компьютерной информации, повлекшего модификацию компьютерной информации, совершенного из корыстной заинтересованности, с использованием своего служебного положения.

Виновная, на основании приказа директора Пензенского регионального филиала АО «Россельхозбанк» принята на должность экономиста, затем переведена на должность ведущего клиентского менеджера.

Осужденная, в соответствии с положениями Инструкции по предоставлению кредитов обладала правами доступа к электронной системе, согласно которым имела функциональные полномочия по вводу данных.

В соответствии должностной инструкции, в обязанности виновной входило: осуществление первоначального ввода параметров кредитной сделки и договоров обеспечения к кредитной сделке; внесение дополнительных реквизитов параметров кредитной сделки и договоров обеспечения; осуществление формирования и печати кредитных сделок, договоров залога и поручительства, проверки договоров на соответствие типовым формам, утвержденным коллегиальным органом Банке и другое.

Также виновная в ходе своей трудовой деятельности была ознакомлена с Инструкцией по соблюдению коммерческой тайны в АО «Россельхозбанк».

Так, виновная, находясь на своем рабочем месте, без обращения клиента ФИО, не имея заявления и согласия клиента на заключение кредитного соглашения, обработку персональных данных, получение его кредитной

истории из бюро кредитных историй, на уступку Банком прав требований, возникающих из Кредитного договора, любому третьему лицу, применяя предоставленные ей в силу служебных полномочий логин и персональный пароль, осуществила вход в компьютерную программу, тем самым преодолев средства защиты, и осуществила в программе ввод и регистрацию заявки от имени ФИО на получение кредита в сумме 25 000 рублей, то есть, произведя без присутствия и согласия клиента Банка ввод и модификацию компьютерной информации, выраженную в создании и регистрации в системе новой заявки на получение кредита, которая содержала персональные данные клиента Банка, и согласно которой последняя обратилась в банк с целью получения кредита в сумме 25 000 рублей.

Таким образом, виновная, имея в силу возложенных на нее трудовым договором и должностной инструкцией полномочий, осуществила неправомерный доступ к охраняемой законом компьютерной информации.[162]

Приговором Ленинского районного суда г. Владикавказа № 1-356/2017 1-44/2018 от 14 февраля 2018 г. по делу № 1-356/2017, лицо признано виновным в совершении преступлений, предусмотренных ч.3 ст.272, ч.2 ст.138 УК РФ. То есть, в совершении неправомерного доступа к охраняемой законом компьютерной информации, повлекшего копирование компьютерной информации, с использованием своего служебного положения, а также нарушении тайны телефонных переговоров граждан, с использованием своего служебного положения.

Так, виновная на основании трудового договора принята в офис продаж на должность помощника с испытательным сроком 3 месяца, затем переведена на должность специалиста офиса продаж.

Виновная, находясь на своем рабочем месте, руководствуясь мотивом личной заинтересованности, выразившейся в желании обладать сведениями о частной жизни потерпевшей, вопреки требованиям должностной инструкции и

[162] Приговор Ленинского районного суда г. Пензы № 1-145/2019 от 17 июля 2019 г. по делу № 1-145/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

трудового договора, согласно которых она обязана соблюдать меры безопасности, направленные на защиту конфиденциальности сведений об абонентах, в отсутствии судебного решения и иных законных оснований, под своей учетной записью и паролем умышленно сформировала в информационной системе системный запрос (заявку) на получение детализации телефонных соединений абонентского номера, используемого потерпевшей.

Так, виновная, имея в силу возложенных на нее трудовым договором и должностной инструкцией полномочий, осуществила неправомерный доступ к охраняемой законом компьютерной информации.[163]

Таким образом, под использованием служебного положения следует понимать использование возможности доступа к компьютерной информации, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ, то есть тех, кто на законных основаниях использует компьютерную информацию и средства ее обращения

Частью 4 ст. 272 УК РФ предусмотрена ответственность за деяния предусмотренные частями первой, второй или третьей, если они повлекли тяжкие последствия или создали угрозу их наступления.

Понятие «тяжкие последствия» в диспозиции статьи не раскрывается, является оценочным и определяется судом в каждом конкретном случае в зависимости от обстоятельств дела.

Под тяжкими последствиями как разновидностью отягчающих наказание обстоятельств следует понимать вызванные преступлением вредные изменения в общественных отношениях (имущественного, физического, морального или иного характера), выходящие за пределы состава преступления. [164]

---

[163] Приговор Ленинского районного суда г. Владикавказа № 1-356/2017 1-44/2018 от 14 февраля 2018 г. по делу № 1-356/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[164]Оценочные признаки в Уголовном кодексе Российской Федерации: научное и судебное толкование [Электронный ресурс]: науч.-практ. пособие / под ред. А. В. Галаховой. – Москва : Норма. – 2014. – Режим доступа: http://www.consultant.ru.

В данном случае дополнительным факультативным объектом выступят различные общественные отношения, в зависимости от наступивших последствий либо последствий которые, могли наступить вследствие совершения преступления, предусмотренного ст. 272 УК РФ.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», в статье 273 УК РФ, тяжесть последствий должна определяться с учетом всей совокупности обстоятельств дела (причинение особо крупного материального ущерба, серьезное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти, уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и др.).

Однако данный акт не раскрывает того, что понимать под тяжкими последствиями применительно к ч. 4 ст. 272 УК РФ.

По нашему мнению, не все из указанных в Методических рекомендациях тяжкие последствия будут полностью охватываться ч. 4 ст. 272 УК РФ.

Так, Г.Н. Хлупина указывает на то, что в Уголовном кодексе имеется достаточное количество преступлений, в состав которого включен признак наступление тяжких последствий, однако описания данного признака в законе нет, он не конкретизирован. При сравнении общественной опасности составного преступления и конкретного отдельно преступления (преступления-элемента), которое входит в составное преступление, необходимо отметить, что выше общественная опасность всегда у составного преступления. Именно по санкции нормы необходимо судить о степени общественной опасности преступления. Исходя из этого, в составном преступлении санкция всегда строже, чем санкция отдельного преступления (преступления-элемента).[165]

[165] Хлупина Г.Н. Квалификация нескольких преступлений : учебное пособие / Г. Н. Хлупина. – Красноярск : ИПК СФУ, 2009. С. 26.

Следовательно, по нашему мнению, причинение тяжкого вреда здоровью, смерти, а также иные наступившие последствия, являющиеся преступлениями, предусмотренными статьями УК РФ, санкция за которые строже, чем предусмотренная за составное преступление, не может охватываться частью 4 ст. 272 УК РФ и такие последствия должны быть квалифицированы по совокупности.

В случае, когда особо крупный материальный ущерб причиняется преступлением, объектом которого выступает собственность (такие как мошенничество или кража) такие действия должны квалифицироваться по совокупности. Это подтверждается позицией Пленума Верховного суда, а также судебной практикой. Так, к примеру, согласно Постановлению Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации требует дополнительной квалификации по статье 272 УК РФ. Таким образом, такие деяния, совершенные посредством неправомерного доступа, не могут охватываться ч. 4 ст. 272 УК РФ.

Один из примеров квалификации неправомерного доступа к компьютерной информации, повлекшего тяжкие последствия, можно проследить в судебной практике.

Так, апелляционным постановлением Московского городского суда от 15 июня 2016 г. по делу № 10-7792/16 на постановление Тверского районного суда города Москвы от 12 апреля 2016 года, которым возвращено Тверскому межрайонному прокурору города Москвы уголовное дело, установлено, что лицу предъявлено обвинение в неправомерном доступе к охраняемой законом компьютерной информации, повлекшем копирование компьютерной информации, совершенном из корыстной заинтересованности, с использованием своего служебного положения, повлекшее тяжкие последствия и угрозу их наступления.

Виновный – частный детектив создал условия для совершения, затем

совершил неправомерный доступ к электронным почтовым ящикам потерпевших, затем скопировал с электронной почты сведения, принадлежащие потерпевшим, и распространил их путем пересылки третьим лицам.

Таким образом, по мнению органов предварительного расследования, тяжкие последствия выразились в том, что действиями обвиняемого, а именно распространением полученных сведений, был причинен ущерб деловой репутации потерпевшего в сфере предпринимательской деятельности, повлекший колоссальные убытки, в связи с чем, риск банкротства увеличился в несколько раз, и ему пришлось искать иные источники дохода. А также, в том, что лицо, являясь частным детективом, распространил полученные частные сведения иных потерпевших (что является нарушением гарантированных Конституцией РФ прав и свобод), что могло повлечь угрозу наступления тяжких последствий.

Принимая решение об оставлении постановления без изменения, суд указал, что ссылка в обвинительном заключении на нарушение гарантированных Конституцией РФ прав и свобод, указанных при описании преступных деяний, свидетельствует о существенном нарушении прав потерпевших действиями обвиняемого, что влечет ответственность в соответствии с ч. 1 ст. 203 УК РФ.

А что касается ст. 272 УК РФ, по мнению суда, квалифицирующий признак «угроза наступления тяжких последствий» в описательной части каждого из событий не раскрыт. Так, при описании преступного деяния необходимо раскрыть, какие конкретно тяжкие последствия могли наступить для потерпевших от инкриминируемых обвиняемому действий, связанных с нарушением их прав и свобод, гарантированных Конституцией РФ. [166]

Таким образом, можно согласиться, что в данном случае тяжкие последствия выразились в нанесении ущерба деловой репутации потерпевшего в сфере предпринимательской деятельности, которое повлекло колоссальные

[166] Апелляционное постановление Московского городского суда от 15 июня 2016 г. по делу № 10-7792/16 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

убытки, в связи с чем, риск банкротства увеличился в несколько раз. Относительно угрозы наступления последствий, действительно, неясно, в чем угроза должна была выразиться и была ли она реальной.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», в ч. 3 ст. 273 УК РФ субъективная сторона характеризуется двумя формами вины – умыслом по отношению к самому деянию и неосторожностью (умысел) по отношению к последствиям. В случае если преступник умышленно относился к наступлению тяжких последствий или созданию угрозы их наступления, то в зависимости от качественной и количественной оценки наступивших тяжких последствий его действия подлежат дополнительной квалификации по совокупности преступлений, предусмотренных соответствующими статьями УК РФ.[167]

Данный акт не раскрывает характеристику субъективной стороны в ч. 4 ст. 272 УК РФ.

Следует отметить, что тяжкие последствия не всегда наступают по неосторожности.

Так, согласно ст. 24 УК РФ, деяние, совершенное только по неосторожности, признается преступлением лишь в случае, когда это специально предусмотрено соответствующей статьей Особенной части настоящего Кодекса.

По нашему мнению, лицо может предвидеть возможность или неизбежность наступления тяжких последствий, желать их наступления, либо сознательно допускать эти последствия, относиться к ним безразлично.

Таким образом, в данном случае субъективная сторона не будет характеризоваться двумя формами вины.

Часть 4 ст. 272 УК РФ также предусматривает ответственность за деяние

[167] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

создавшее угрозу наступления тяжких последствий. В данном случае состав является усеченным, то есть деяние считается оконченным с момента, когда возникает реальная возможность наступления таких последствий.

3 Отграничение преступления, предусмотренного ст. 272 УК РФ, от смежных составов преступлений и иных преступлений.

При решении вопроса о квалификации деяния по ст. 272 УК РФ, необходимо отграничивать неправомерный доступ к компьютерной информации от иных видов преступных посягательств, связанных с уничтожением, блокированием, модификацией либо копированием информации, преступлений, предметом которых является компьютерная информация. Среди таких преступлений:

1) преступления в сфере компьютерной информации:

- ст. 273 УК РФ – создание, использование и распространение вредоносных компьютерных программ;
- ст. 274 УК РФ – нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей;
- ст. 274.1 УК РФ – неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации);

2) ст. 159.6 УК РФ – мошенничество в сфере компьютерной информации;

3) иные преступления, предметом которых может являться компьютерная информация, такие как нарушение авторских и смежных прав (ст. 146 УК РФ), незаконные получение и разглашение сведений, составляющих коммерческую или банковскую тайну (ст. 183 УК РФ) и иные.

Статьи 273, 274, 274.1 УК РФ расположены в главе 28 УК РФ – преступления в сфере компьютерной информации, а, следовательно, родовым объектом, как и в ст. 272 УК РФ, будут признаваться общественные отношения, обеспечивающие общественную безопасность и общественный порядок.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», основной объект преступлений, предусмотренных ст. 273, 274 УК РФ – общественные

отношения, обеспечивающие безопасность в сфере компьютерной информации.[168]

Таким образом, составы преступлений, предусмотренные ст. 272 и 273, 274 УК РФ имеют единый объект.

Статья 273 УК РФ предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Предмет преступления, согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», по содержанию совпадает с предметом преступления, предусмотренного ст. 272 УК РФ.[169]

Однако, исходя из диспозиции статьи, следует, что защите подлежит компьютерная информация, в отличие от ст. 272 УК РФ, где под защиту ставится охраняемая законом компьютерная информация.

Таким образом, в ст. 273 УК РФ защите подлежит любая информация, то есть как охраняемая законом, так и неохраняемая законом информация. Наличие собственника, владельца значения не имеет. Также для квалификации не важно, предназначена ли была такая информация для широкого круга лиц.

Следующим признаком для разграничения составов является объективная сторона.

Объективная сторона преступления, предусмотренного ст. 273 УК РФ, включает альтернативные действия, состоящие:

1) в создании программ или иной компьютерной информации,

---

[168] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[169] Там же.

заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств ее защиты;

2) в распространении таких программ, иной компьютерной информации;

3) в использовании таких программ, иной компьютерной информации.

Создание программ представляет собой деятельность, направленную на разработку, подготовку программ, способных по своему функционалу несанкционированно уничтожать, блокировать, модифицировать, копировать компьютерную информацию или нейтрализовать средства защиты компьютерной информации.

Под распространением таких программ понимается предоставление доступа к ним любому постороннему лицу любым из возможных способов, включая продажу, прокат, бесплатную рассылку по электронной сети, то есть любые действия по предоставлению доступа к программе сетевым или иным способом.

Использование программы – это работа с программой, применение ее по назначению и иные действия по введению ее в хозяйственный оборот в изначальной или модифицированной форме. Под использованием вредоносных программ понимается их применение (любым лицом), при котором активизируются их вредные свойства.[170]

Рассматриваемое преступление будет считаться оконченным с момента создания, использования или распространения таких программ или информации, создающих угрозу наступления указанных в законе последствий, вне зависимости от того, наступили реально последствия или нет. Состав преступления является формальным. Напротив, состав преступления,

[170] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

предусмотренного ст. 272 УК РФ является материальным, и считается оконченным с момента наступления указанных в законе последствий.

Субъективная сторона состава преступления, предусмотренного ч. 1 ст. 273 УК РФ, характеризуется виной в виде прямого умысла. При этом виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к указанным в законе общественно опасным последствиям. Субъективная сторона неправомерного доступа к компьютерной информации, характеризуется виной в виде прямого, косвенного умысла или неосторожности.

Субъект преступления общий – вменяемое лицо, достигшее шестнадцати лет.

Таким образом, составы преступлений, предусмотренных статьями 272 и 273 УК РФ, различаются по таким признакам как предмет, объективная сторона и субъективная сторона.

Так, приговором Кирсановского районного суда (Тамбовской области) № 1-140/2019 от 28 августа 2019 г. по делу № 1-140/2019, установлено, что виновный решил воспользоваться специализированной компьютерной программой, предназначенной заведомо для него для нейтрализации средств защиты компьютерной информации, использование которой может повлечь несанкционированное уничтожение, блокирование, модификацию, копирование компьютерной информации на сервере. Виновный запустил компьютерную программу и применил механизм ее работы в отношении интернет-ресурса, принадлежащего Государственному бюджетному учреждению культуры «Государственный историко-архитектурный художественный и ландшафтный музей-заповедник «Царицыно».

Действия виновного суд квалифицировал по ч. 1 ст. 273 УК РФ – использование компьютерной программы, заведомо предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации и нейтрализации средств защиты

компьютерной информации.[171]

Если лицо создало, распространило или использовало вредоносные компьютерные программы либо иную компьютерную информацию, и с их помощью осуществило неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение, блокирование, модификацию и копирование такой информации, деяние следует квалифицировать по совокупности.

Так, приговором Центрального районного суда г. Челябинска № 1-297/2019 от 17 июня 2019 г. по делу № 1-297/2019 установлено, что виновный перечислил на указанный неустановленным лицом Qiwi кошелёк денежные средства в сумме 1 000 рублей, за приобретение вредоносной компьютерной программы. После совершения лицом указанных действий, неустановленное лицо, предоставило виновному право осуществлять авторизации к Интернет-ресурсу, на котором находилась вредоносная компьютерная программа.

Далее, виновный, во исполнение своего преступного умысла, направленного на использование компьютерной программы, заведомо предназначенной для несанкционированного копирования компьютерной информации, создал раздел, на котором разместил неустановленные в ходе следствия видео файлы. После чего умышленно, преследуя цель обманным путём осуществить использование на компьютерах пользователей вредоносной компьютерной программы, разместил под данными видео файлами ссылку, которая позволяла пользователям автоматически осуществлять копирование файла, содержащего вредоносную компьютерную программу.

Кроме того, виновный совершил неправомерный доступ к хранящейся на компьютере охраняемой законом компьютерной информации – паролям и логинам, принадлежащим потерпевшим, повлекший копирование компьютерной информации.

Потерпевшие, не осведомлённые о преступных намерениях виновного, в

[171] Приговор Кирсановского районного суда (Тамбовской области) № 1-140/2019 от 28 августа 2019 г. по делу № 1-140/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

ходе просмотра размещённого виновным видео, перешли по расположенной под видео ссылке, тем самым осуществили копирование на принадлежащие им персональные компьютеры файлов, содержащих компьютерную программу, предназначенную для несанкционированного копирования компьютерной информации. После чего произошла установка данной программы. При этом указанная компьютерная программа без ведома потерпевших обнаружила в автоматическом режиме на браузерах логино-парольные комбинации и url-адреса веб-сайтов, необходимые для авторизации на Интернет-ресурсах.

Своими действиями виновный совершил преступление, предусмотренное ч. 1 ст. 273 Уголовного кодекса Российской Федерации – использование компьютерных программ, заведомо предназначенных для несанкционированного копирования компьютерной информации, а также преступление, предусмотренное ч. 1 ст. 272 УК РФ – неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее копирование.[172]

Составы преступлений, отличающиеся по одному или нескольким признакам, при совпадении остальных являются смежными.

Отличающиеся признаки могут быть нейтрального, а могут быть противоположного, взаимоисключающего характера.

В случае если смежные преступления имеют несовпадающие признаки, которые носят либо противоположный, либо взаимоисключающий характер, несовпадающие признаки являются несовместимыми. Несовместимость признаков означает, что в общественно опасном деянии могут быть признаки только одного смежного преступления, идеальная совокупность невозможна.

Большинство преступлений, исходя из анализа составов, отличаются друг от друга по двум и более признакам, таких как объект, предмет объективная и субъективная стороны.[173]

Таковыми являются ст. 272 УК РФ и ст. 274 УК РФ.

---

[172] Приговор Центрального районного суда г. Челябинска № 1-297/2019 от 17 июня 2019 г. по делу № 1-297/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

[173] Иногамова-Хегай Л.В Концептуальные основы конкуренции уголовно-правовых норм [Электронный ресурс] : монография / Л.В. Иногамова-Хегай – Москва : Норма, Инфра-М, 2015. – Режим доступа: http://www.consultant.ru.

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Предметом данного преступления, в соответствии с «Методическими рекомендациями по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование. [174]

По мнению В.Г. Степанова-Егиянца, предметом преступления также признается охраняемая законом компьютерная информация.[175]

К средствам хранения, обработки или передачи компьютерной информации В.Г. Степанов-Егиянц относит различные электронные устройства, способные хранить и обрабатывать компьютерную информацию. Среди них ПК, карты памяти, USB-носители (флеш-карты), дискеты, диски.[176]

Статья 2 ФЗ «Об информации, информационных технологиях и о защите информации» определяет информационно-телекоммуникационную сеть как технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники.[177]

---

[174] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[175] Степанов-Егиянц В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В. Г. Степанов-Егиянц – Москва : Статут, 2016. – Режим доступа: http://www.consultant.ru.

[176] Там же.

[177] Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

В соответствии со ст. 2 ФЗ «О связи», оконченное оборудование (пользовательское оборудование) – это технические средства для передачи и приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.[178]

Предметом преступления, предусмотренного ст. 272 УК РФ является охраняемая законом компьютерная информация.

Также, признаком для разграничения составов является объективная сторона.

Объективная сторона преступления, предусмотренного ст. 274 УК РФ, состоит в нарушении правил хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, если такое нарушение повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб.

Предполагается, что состав преступления связан как с правомерным воздействием на средства хранения информации, так и неправомерным. При неправомерном доступе к компьютерной информации виновный не имеет права доступа, следовательно, действует неправомерно.

Данная норма, предусмотренная в ч. 1 ст. 274 УК РФ, является бланкетной. Необходимо обращаться к конкретным инструкциям и правилам, которые регламентируют порядок работы со средствами хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационными сетями и оконечным оборудованием.[179]

Такие правила должны быть направлены на обеспечение безопасности

---

[178] О связи [Электронный ресурс] : федер. закон от 07.07.2003 № 126-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[179] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

информации.

Согласно Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации, такие правила предусмотрены в различных ГОСТах, инструкциях, уставах, положениях и приказах, договорах соглашениях, иных документах, содержащих правила доступа к информации и эксплуатации оборудования.[180]

Можно привести некоторые примеры нарушения правил эксплуатации:

- нарушение правил безопасности средств хранения, обработки и передачи информации, сетей и оконечного оборудования;

-несоблюдение либо ненадлежащее соблюдение правил.[181]

Между фактом нарушения и наступившими последствиями должна быть установлена причинная связь, а также доказано, что наступившие последствия являются результатом нарушения правил эксплуатации, а не ошибкой либо деяниями, предусмотренными ст. 272 и 273 УК РФ.[182]

Если последствия наступили вследствие неправомерного доступа к компьютерной информации, то такое деяние должно быть квалифицировано по ст. 272 УК РФ. Совокупность преступлений может возникнуть если последствия наступили вследствие совершения разных деяний – неправомерного доступа и нарушения правил эксплуатации, то есть имела место реальная совокупность.

Так, приговором Кировградского городского суда № 1-105/2016 от 5 августа 2016 г. по делу № 1-105/2016 установлено, что виновный совершил нарушение правил эксплуатации средств хранения, обработки, передачи компьютерной информации при следующих обстоятельствах, то есть

---

[180] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

[181] Степанов-Егиянц В. Г. Указ. соч.. – Режим доступа: http://www.consultant.ru.

[182] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

преступление, предусмотренное ч. 1 ст. 274 УК РФ. А также в совершении преступлений, предусмотренных ч. 2 ст. 273, ч. 2 ст. 272, ч. 2 ст. 159.6.

Виновный, согласно установленным обстоятельствам, имея цель нарушения правил эксплуатации терминала (средства хранения, обработки и передачи информации), установил в его систему вредоносную компьютерную программу для последующего хищения денежных средств.

В соответствии с пунктом 1.3 Положения Центрального Банка РФ от 24.12.2004 года № 266 – П «Об эмиссии платёжных карт и об операциях, совершаемых с их использованием», терминал является устройством самообслуживания и средством хранения охраняемой законом информации. В данном устройстве формируется электронный журнал, электронный документ, содержащий данные об операциях. В соответствии с данным актом, терминал эксплуатируется клиентом с помощью использования денежных средств либо платежных карт.

Зная о порядке работы терминала, виновный совершил неправомерный доступ к компьютерной информации, с целью получения возможности осуществлять контроль над работой терминала, нанося ущерб Банку, внес в систему терминала вредоносную программу, которую в дальнейшем запустил.

В результате описанных действий, произошла такая модификация операционной системы терминала, которая выразилась в подключении вредоносной компьютерной программы к порту купюроприемника. Так, виновный получил возможность управления движением денежных средств банка.

Таким образом, виновный осуществил хищение денежных средств на сумму 1 021 000 рублей, что привело к причинению банку крупного ущерба.[183]

В данном случае, суд квалифицировал деяние лица по нескольким статьям, что является неверным. Хищение денежных средств произошло не вследствие нарушений правил эксплуатации средства хранения информации, а

[183] Приговор Кировградского городского суда № 1-105/2016 от 5 августа 2016 г. по делу № 1-105/2016 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

в результате использования вредоносной компьютерной программы, которая обеспечила возможность неправомерного доступа к охраняемой законом компьютерной информации, что и повлекло ее модификацию и причинение крупного ущерба.

Таким образом, осуждение лица по ст. 274 УК РФ является незаконным и излишним.

В соответствии с «Методическими рекомендациями по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», нарушение правил эксплуатации и доступа может совершаться как умышленно, так и по неосторожности.[184]

При этом умысел лица должен быть направлен на нарушение правил эксплуатации, при неправомерном доступе к компьютерной информации умысел должен быть направлен на осуществление доступа к охраняемой законом компьютерной информации.

Состав преступления, предусмотренный ст. 274 УК РФ, является материальным. Преступление считается оконченным при наступлении одного из последствий, перечисленных в диспозиции нормы – уничтожение, блокирование, модификация либо копирование компьютерной информации. Одновременно эти деяния должны повлечь причинение крупного ущерба.

Таким образом, составы преступлений, предусмотренных статьями 272 и 274 УК РФ, различаются по таким признакам как предмет, объективная сторона и субъективная сторона.

Часть 2 ст. 274.1 Уголовного кодекса Российской Федерации предусматривает ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием

[184] Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

Говоря, об объекте преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, им необходимо признать отношения безопасности критической информационной инфраструктуры Российской Федерации, а именно состояние защищенности от различного рода воздействий техническими и программными устройствами и средствами, способное нарушить функционирование инфраструктуры и безопасность информации, которая обрабатывается ей.[185]

Предметом преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, является охраняемая законом компьютерная информация, которая содержится в критической информационной инфраструктуре Российской Федерации.

В соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации», объекты критической информационной инфраструктуры должны быть отражены в Реестре значимых объектов критической информационной инфраструктуры.[186]

Под объектами критической информационной инфраструктуры обычно понимаются различные информационные, информационно-телекоммуникационные, автоматизированные системы и сети, а также системы управления технологическими процессами, принадлежащие органам государственной власти и государственным органам, либо функционирующие в различных областях, таких как оборонная, атомная, топливная, горнодобывающая, химическая промышленность, энергетика, здравоохранение, транспорт, связь, кредитно-финансовая сфера, ракетно-

[185] Решетников А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) [Электронный ресурс] / А. Ю. Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

[186] О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : федер. закон от 26.07.2017 № 187-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

химическая и металлургическая промышленность.[187]

Часть 2 ст.274.1 и ст. 272 УК РФ разграничиваются также по объективной стороне.

Объективная сторона преступления, предусмотренного ч. 2 ст. 274.1 УК РФ – неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре.

Состав преступления – материальный. Преступление считается оконченным при причинении вреда критической информационной инфраструктуре Российской Федерации.

Сам по себе неправомерный доступ как в ст. 272 УК РФ, так и в ч. 2 ст. 274.1 УК РФ не является преступлением. В случае, если лицу, которое осуществило неправомерный доступ к компьютерной информации, содержащейся в критической информационной инфраструктуре, однако, по не зависящим от него обстоятельствам не удалось причинить вред критической информационной инфраструктуре Российской, содеянное следует квалифицировать как покушение на преступление, предусмотренное ч. 2 ст. 274.1 УК РФ, то есть по ч. 3 ст. 30 и ч. 2 ст. 274.1 УК РФ.[188]

Статья 272 УК РФ предусматривает последствия в виде блокирования, копирования, модификации, уничтожения охраняемой законом компьютерной информации.

Вред является обязательным признаком состава преступления, предусмотренного ч. 2 ст. 274.1 УК РФ. Однако что подразумевается под вредом, и что считать вредом, причиненным информационной структуре РФ, закон не раскрывает.

По мнению А.Ю. Решетникова, Е.А. Русскевича, и исходя из системного толкования УК РФ, вред заключается в уничтожении, блокировании, модификации, копировании информации, содержащейся в критической

[187] Решетников А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) [Электронный ресурс] / А. Ю. Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

[188] Там же.

информационной инфраструктуре. Помимо этого в него включается нейтрализация и преодоление средств защиты такой информации или выведение из строя, поломка информационно-технических средств, благодаря которым функционирует критическая информационная инфраструктура. Деяние следует квалифицировать по ч. 5 ст. 274.1 УК РФ, если вред, который наступил вследствие неправомерного доступа к компьютерной информации, содержащейся в критической информационной инфраструктуре, повлек наступление тяжких последствий.[189]

Таким образом, объективная сторона данных преступлений совпадает в случае неправомерного доступа, повлекшего копирование, блокирование, модификацию и уничтожение информации, если же наступили иные последствия, выразившиеся причинении вреда критической информационной инфраструктуре, объективная сторона преступлений будет различна.

Субъектом преступления, предусмотренного ч. 2 ст. 274.1 УК РФ, является физическое вменяемое лицо, достигшее возраста 16 лет.

Субъективная сторона преступления выражается в умышленной форме вины в виде прямого и косвенного умысла.

Таким образом, составы преступлений, предусмотренных статьями 272 и ч. 2 ст. 274.1 УК РФ, различаются по таким признакам как непосредственный объект и предмет преступления. Анализируемая уголовно-правовая норма конкурирует со ст. 272 УК РФ и является специальной по отношению к ней. Ответственность за совершение преступления, предусмотренного ч. 2 ст. 274.1 наступает в случае неправомерного доступа к охраняемой законом компьютерной информации, содержащейся в критической информационной инфраструктуре, повлекшее уничтожение, блокирование, модификацию и копирование такой информации, то есть причинившего вред критической информационной инфраструктуре Российской Федерации.

---

[189] Решетников А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) [Электронный ресурс] / А. Ю. Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

На практике при квалификации деяний существуют трудности применения норм, предусмотренных ст. 159.6 и 272 УК РФ.

Статья 159.6 УК РФ предусматривает ответственность за мошенничество в сфере компьютерной информации, то есть 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.

Статья 159.6 находится в главе 21 УК РФ – преступления против собственности.

Непосредственным объектом данного преступления являются отношения собственности. Предмет преступления – чужое имущество.[190]

Дополнительным объектом преступления, предусмотренного ст. 159.6 являются общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу. Наоборот, при неправомерном доступе к компьютерной информации, совершенном из корыстной заинтересованности, непосредственным объектом выступают общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

Объективную сторону мошенничества в сфере компьютерной информации составляет хищение чужого имущества или приобретение права на чужое имущество.

Ввод, удаление, блокирование, модификация компьютерной информации либо иное вмешательство в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей являются способами совершения преступления, предусмотренного ст. 159.6 УК РФ. При неправомерном доступе к

[190] Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [Электронный ресурс] / под ред. А. В. Бриллиантова. – Режим доступа: http://www.consultant.ru.

компьютерной информации уничтожение, блокирование и модификация являются обязательными последствиями преступления.

Субъект преступления общий – вменяемое физическое лицо, достигшее 16 лет.

Субъективная сторона преступления предполагает прямой умысел.

В данном случае, умысел направлен на хищение имущества или завладение правом на имущество. Наоборот, при неправомерном доступе, совершаемом из корыстной заинтересованности, умысел направлен на получение такой информации и сведений, обладание которыми будет способствовать для виновного получению выгоды имущественного характера.

Преступление, предусмотренное ст. 159.6 УК РФ является преступлением с материальным составом, обязательным условием его совершения выступает хищение чужого имущества или приобретение права на чужое имущество.[191]

В соответствии с Постановлением Пленума Верховного суда от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате», мошенничество в сфере компьютерной информации, совершенное посредством неправомерного доступа к компьютерной информации требует дополнительной квалификации по статье 272 УК РФ.[192]

Следовательно, если лицо, завладев чужим имуществом, или правом на чужое имущество на законных основаниях осуществило доступ к компьютерной информации, что повлекло удаление, блокирование, модификацию и иные последствия, дополнительной квалификации по с. 272 УК РФ не требуется.

Согласно позиции С.В. Шевелевой, при решении вопроса о совокупности преступлений со статьей 272 УК РФ, необходимо учитывать несколько условий. Во-первых, необходимо в каждом случае выяснять основания доступа к компьютерной информации. И, во-вторых, если доступ несанкционирован,

---

[191] Елин В. М. Мошенничество в сфере компьютерной информации как новый состав преступления [Электронный ресурс] / В. М. Елин // Бизнес-информатика. – 2013. – № 2. – Режим доступа: http://cyberleninka.ru

[192] О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

квалификацию необходимо осуществлять, исходя из правил о единстве родового объекта, а также основываясь на категории преступлений.[193]

Так, необходимо учитывать нормы Общей части УК РФ. В соответствии со ст. 17 УК РФ, совокупность преступлений исключается, когда совершение двух или более преступлений предусмотрено статьями Особенной части УК РФ в качестве обстоятельства, влекущего более строгое наказание.

Учитывая, что часть 1 статьи 159.6 УК РФ относится с категории преступлений небольшой тяжести и предусматривает менее строгую ответственность, то следуя правилам квалификации, необходимо дополнительно квалифицировать содеянное по соответствующей статье УК РФ, которая отношению к статье 159.6 УК РФ является способом ее совершения, вне зависимости от того, совпадают ли родовые объекты или нет.

При мошенничестве, совершаемом посредством неправомерного доступа к компьютерной информации, необходима квалификация по ст. 272 УК РФ.

Так, Постановлением от 14 февраля 2019 г. № 44у-36,37/2019 Президиума Самарского областного суда, Приговор Автозаводского районного суда г. Тольятти Самарской области от 12 сентября 2018 года и апелляционное определение судебной коллегии по уголовным делам Самарского областного суда от 6 ноября 2018 года в отношении виновного отменены.

Виновному, органами следствия на этапе предварительного расследования, предъявлено обвинение в совершении неправомерного доступа к охраняемой законом компьютерной информации, что повлекло модификацию компьютерной информации, с использованием своего служебного положения, то есть в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, а также мошенничества в сфере компьютерной информации, то есть хищения чужого имущества путем модификации компьютерной информации, с использованием своего служебного положения, то есть в совершении преступления, предусмотренного ч. 3 ст. 159.6 УК РФ.

---

[193] Шевелева С. В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами[Электронный ресурс] / С. В. Шевелева // Юридическая наука и практика: Вестник Нижегородской академии МВД России. – 2017. – № 4. – Режим доступа: http://cyberleninka.ru

Приговором Автозаводского районного суда г. Тольятти Самарской области от 12 сентября 2018 года лицо признано виновным в совершении мошенничества в сфере компьютерной информации, а именно хищении денежных средств организации путем модификации компьютерной информации и осужден по ч. 1 ст. 159.6 УК РФ. Обвинение лица по ч. 3 ст. 272 УК РФ исключено как излишне вмененное.

Принимая решение, суд указал, что в действиях лица отсутствуют признаки состава преступления, предусмотренного ч. 3 ст. 272 УК РФ, поскольку его действия полностью охватываются ч. 1 ст. 159.6, и следовательно дополнительная квалификация привела бы к двойному учету одного и того же деяния. В описательно-мотивировочной части решения суд пояснил, что умысел лица был направлен именно на завладение денежными средствами организации путем неправомерного доступа, и, таким образом, составили объективную сторону преступления, предусмотренного статьей 159.6 УК РФ.

Прокурор внес кассационное представление, в котором не согласился с приговором суда и апелляционным определением судебной коллегии, по его мнению, содеянное должно быть квалифицировано по совокупности ч. 1 ст. 159.6 и ч. 3 ст. 272 УК РФ. Так, исходя из установленных обстоятельств дела, виновный совершил неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее модификацию в программе, принадлежащей организации, при этом используя информацию об абонентских номерах, получил возможность распоряжаться их счетами в данной организации, то есть, таким образом, совершил преступление, предусмотренной статьей 272 УК РФ. Далее, используя, возможность по распоряжению средствами абонентов на их лицевых счетах, осуществил перевод этих средств, то есть их хищение.

Рассматривая дело, суд кассационной инстанции пришел к выводу о том, что данные преступления предусматривают ответственность за совершение различных преступлений, так как имеют различную объективную сторону. Суд, соглашаясь с мнением прокурора, указал, что, действительно, виновный

изначально совершил модификацию компьютерной информации путем неправомерного доступа к программе организации, что таким образом дало ему возможность распоряжения денежными средствами абонентов. Затем осуществил хищение денежных средств с лицевых счетов, путем перевода денежных средств в данной программе на свой счет, то есть совершил мошенничество в сфере компьютерной информации.[194]

Таким образом, по нашему мнению, квалификация по совокупности преступлений в данном случае является правильной, поскольку, во-первых, признак неправомерности доступа к охраняемой законом компьютерной информации статьей 159.6 УК РФ не предусмотрен, а во-вторых, статья 159.6 УК РФ не предусматривает более строгое наказание за совершение хищения и блокирования, модификации и других действий, а, следовательно, принцип справедливости, согласно которому не допускается двойная ответственность за одно деяние, не нарушается.

Так же, необходимо правильно квалифицировать деяния, связанные с неправомерным доступом к охраняемой законом компьютерной информации, то есть такие деяния, последствием которых является уничтожение, блокирование, модификация либо копирование компьютерной информации, и, предметом которых является компьютерная информация. Так, в российском уголовном законодательстве предусмотрен ряд статей, связанных с посягательствами на информацию граждан, доступ к которой ограничен: ст. 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений); ст. 146 УК РФ (Нарушение авторских и смежных прав); ст. 147 УК РФ (Нарушение изобретательских и патентных прав); ст. 183 УК РФ (Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну); ст. 283.1 (Незаконное получение сведений, составляющих государственную тайну) и другие.

---

[194] Постановление Президиума Самарского областного суда от 14 февраля 2019 г. № 44у-36,37/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

В случае совершения таких преступлений посредством неправомерного доступа к компьютерной информации, деяние следует квалифицировать по совокупности преступлений, предусмотренных ст. 272 УК РФ и преступлений, предусмотренных соответствующими статьями Уголовного Кодекса.

Приговором Золотухинского районного суда Курской области № 1-28/2018 от 23 мая 2018 г. по делу № 1-28/2018, лицо признано виновным в совершении преступлений, предусмотренных частью 1 статьи 159.6, частью 3 статьи 183, частью 3 статьи 272 УК РФ. А именно мошенничество в сфере компьютерной информации, незаконное использование сведений, составляющих коммерческую тайну, без согласия их владельца, лицом, которому она стала известна по работе, совершенное из корыстной заинтересованности, а также неправомерный доступ к охраняемой законом компьютерной информации, повлекший ее модификацию, с использованием своего служебного положения.

Так, виновный осуществил неправомерный доступ к компьютерной информации системы ФГУП «Почта России», касающейся денежных переводов лиц, являющейся коммерческой тайной. Зная имена отправителей и получателей, без их согласия сформировал в системе квитанции о переводах денежных средств на различные суммы от 6 до 9 тысяч рублей, используя ложные паспортные данные. Затем, используя сформированные квитанции, получил на их основании из кассы денежную сумму в размере 24500 рублей.[195]

Так, приговором Ленинградского районного суда Краснодарского края № 1-110/2019 от 27 августа 2019 г. по делу № 1-110/2019, лицо признано виновным в совершении преступлений, предусмотренных ч. 3 ст. 272 УК РФ, ч. 2 ст. 138 УК РФ. То есть неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло копирование компьютерной информации, совершенное лицом с использованием своего служебного положения, а также нарушение тайны телефонных переговоров и иных сообщений граждан, совершенное лицом с использованием своего

[195] Приговор Золотухинского районного суда Курской области № 1-28/2018 от 23 мая 2018 г. по делу № 1-28/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

служебного положения.

Виновный, являясь на основании приказа (распоряжения) директора Краснодарского филиала ПАО «Вымпел-Коммуникации», специалистом обслуживания и продаж, имея доступ к охраняемой законом информации, а также умысел на совершение неправомерного доступа к охраняемой законом компьютерной информации по мотивам личной заинтересованности, сохранил детализацию телефонных переговоров абонента, чем совершил копирование охраняемой законом компьютерной информации.

Также, в нарушение должностной инструкции специалиста офиса ПАО «Вымпел-Коммуникации», порядка обращения с информацией ограниченного доступа, нормативно-правовых актов Российской Федерации, имея умысел на совершение нарушения тайны телефонных переговоров лицом с использованием своего служебного положения, по мотивам личной заинтересованности, а также в нарушение порядка предоставления персональных данных, регламентированного федеральным законодательством, без согласия абонента, предоставил третьим лицам детализацию телефонных переговоров абонента.[196]

Учитывая, что способом совершения таких преступлений чаще всего выступает копирование компьютерной информации, то необходимо отметить следующее.

Копирование описывается такими признаками составов как: «собирание», «присвоение», «приобретение», «получение», «изъятие» и др. Однако, закрепление в ст. 272 УК РФ самостоятельного последствия в виде копирования не охватывается данными составами и требует квалификации по совокупности преступлений.

Ранее, нами был сделан вывод о том, что сложившуюся практику вряд ли можно назвать приемлемой. По нашему мнению, она приводит к неправильной излишней квалификации одного деяния по двум статьям и как следствие к

[196] Приговор Ленинградского районного суда Краснодарского края № 1-110/2019 от 27 августа 2019 г. по делу № 1-110/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

двойной ответственности за преступление, что противоречит принципу справедливости, предусмотренному ч. 2 ст. 6 УК РФ. Следовательно, исключение из диспозиции статьи 272 УК РФ признака – копирование компьютерной информации, который не несет в себе общественной опасности, равноценной другим последствиям, по нашему мнению повлечет за собой правильную оценку деяний, связанных с посягательствами на информацию граждан, доступ к которой ограничен.

Таким образом, необходимо отграничивать преступление, предусмотренное ст. 272 УК РФ и иные смежные составы, другие преступления. Это является немаловажным вопросом при квалификации деяния. Разграничивать такие составы необходимо, прежде всего, по предмету, объективной стороне и направленности умысла виновного, а также другим признакам этих преступлений.

ЗАКЛЮЧЕНИЕ

Таким образом, Уголовное законодательство содержит норму, предусматривающую ответственность за неправомерный доступ к компьютерной информации, повлекший уничтожение, копирование, блокирование либо модификацию такой информации.

Необходимо выделить следующие выводы проведенного исследования.

1) Согласно Уголовному кодексу компьютерная информация, являющаяся предметом исследуемого преступления, должна быть представлена в форме электрических сигналов. Термин «электрический сигнал» является техническим, и определение этого признака находит отражение в таких науках как информатика и физика. Однако понятие «электрического сигнала» при его трактовке с точки зрения физики и информатики отличается, в связи с чем имеют место проблемы в его понимании правоприменителем, и, следовательно, необходимо его разъяснение или замена.

По нашему мнению, следует отказаться от указания на «электрические сигналы», поскольку разъяснение технических терминов в законодательстве создаст еще больше трудностей в применении нормы. Так, под компьютерной информацией должны пониматься сведения, представленные в электронно-цифровой форме (то есть пригодные для восприятия человеком, передачи по каналам связи, обработки в информационных системах), независимо от средств их хранения, обработки и передачи.

2) Поскольку предметом преступления является компьютерная информация, возникает вопрос, где находится эта информация. Уголовный закон говорит нам о том, что под такой информацией понимаются сведения, вне зависимости от средств хранения, обработки и передачи. Однако в науке не утихают споры о том, что необходимо обозначить в законе факт нахождения информации на материальном носителе.

По нашему мнению, вводить в определение понятие «компьютерная информация» нахождение информации на каком-либо материальном носителе

нецелесообразно. Так, компьютер не является единственным средством хранения и обработки информации, и перечислить все средства в законе невозможно. Материальных носителей информации достаточно много, и при появлении новых средств хранения и обработки информации возникнет необходимость во внесении изменений в УК РФ. А также внесение в Уголовный кодекс технических терминов в норму, предусматривающую на настоящий момент большое количество таких понятий, может привести к дополнительным проблемам в квалификации по ст. 272 УК РФ.

3) Для правильной квалификации деяния, в том числе по ч. 1 и 3 ст. 30 УК РФ, как приготовление и покушение к преступлению необходимо определить момент начала и окончания деяния в виде неправомерного доступа.

Нами был сделан вывод о том что, началом доступа необходимо признать действия непосредственно направленные на преодоление средств защиты информации и их нейтрализацию (получение логинов и паролей, планирование технической стороны совершения преступления, подыскание специализированных программ для доступа). Моментом окончания доступа будет считаться получение доступа к компьютерной информации, когда лицо имеет возможность осуществлять манипуляции с информацией и воздействовать на нее (ввод паролей, использование программ для получения доступа к информации и другие).

4) Говоря о последствиях данного преступления необходимо выделить следующее.

Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», уничтожение информации – это приведение информации или ее части в непригодное для использования состояние независимо от возможности ее восстановления

По нашему мнению, согласиться с официальным источником не представляется возможным. Так, нельзя говорить об уничтожении информации, если имеется возможность ее восстановить, поскольку если

информация восстанавливаема, то она не уничтожена, а значит, вред объекту не причиняется.

Таким образом, под уничтожением следует понимать приведение информации или ее части в непригодное для использования состояние, при котором восстановить информацию невозможно.

5) Понятие модификации информации также является спорным. Согласно «Методическим рекомендациям по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», модификация информации – это внесение изменений в компьютерную информацию (или ее параметры). Данный источник не конкретизирует, какие именно изменения должны быть внесены, из чего следует вывод, что таковыми могут быть любые изменения.

По нашему мнению, не любое внесение изменений в компьютерную информацию является преступным. Так, изменения, не влекущие негативных последствий для правообладателя, не причиняющие вреда объекту посягательства, не будут являться преступными. Несущественными изменениями, которые не должны признаваться преступными, можно назвать такие как постановка лишних знаков препинания в электронном документе, его переименование, изменение формата документа (сохранение файла в более ранней, поздней версии Word).

6) Одним из важнейших выводов исследования был сделан нами относительно признака копирование компьютерной информации. Так, копирование компьютерной информации не несет в себе такой общественной опасности, которая была бы равноценна модификации, блокированию или уничтожению, то есть иным альтернативным признакам данного преступления. Представляется, что реальную общественную опасность, причиняющую вред объекту, составляет дальнейшее противоправное использование, но не копирование как таковое.

Так, согласно приведенному нами исследованию статистики применения нормы о неправомерном доступе к компьютерной информации, повлекшему ее

копирование, в большинстве случаев суды квалифицируют данное деяние по правилам идеальной совокупности со статьями, предусматривающими ответственность за посягательство на информацию граждан и организаций, доступ к которой ограничен

Соответственно реальное фактическое использование компьютерной информации (которое непосредственно причиняет вред названным общественным отношениям) выражается в совершении иных самостоятельных преступлений, посягающих на иные непосредственные объекты. Копирование компьютерной информации, в указанных случаях, фактически выступает способом совершения других преступлений, оно описывается такими признаками составов как: «собирание», «присвоение», «приобретение», «получение», «изъятие» и др. Тем не менее, закрепление в ст. 272 УК РФ самостоятельного последствия в виде копирования не охватывается данными составами и, соответственно, требует квалификации по совокупности преступлений.

Следовательно, по вышеуказанным причинам, необходимо исключить данный признак – копирование компьютерной информации.

Таким образом, к последствиям данного преступления, предусмотренного ст. 272 УК РФ следует относить уничтожение (в случае если информация не подлежит восстановлению), блокирование и модификацию компьютерной информации (которая влечет существенные изменения документа, влекущие негативные изменения для правообладателя).

В качестве возможного варианта нами предлагается также включить в КоАП состав правонарушения, предусматривающего ответственность за неправомерный доступ к компьютерной информации без указания наступления общественно-опасных последствий. Незаконное копирование следовало бы рассматривать как типичное последствие указанного правонарушения, не причиняющее существенный вред общественным отношениям. А в случае неправомерного дальнейшего использования информации, следует квалифицировать по соответствующим статьям УК РФ. А именно по ст. 138

УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений); ст. 146 УК РФ (Нарушение авторских и смежных прав); ст. 147 УК РФ (Нарушение изобретательских и патентных прав); ст. 183 УК РФ (Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну); ст. 283.1 (Незаконное получение сведений, составляющих государственную тайну) и другим.

7) Наиболее дискуссионным является вопрос определения субъективной стороны преступления, предусмотренного ст. 272 УК РФ.

По нашему мнению, в ст. 272 УК РФ форма вины может выражаться в виде умысла, прямого и косвенного, а также в виде неосторожности. Однако, поскольку состав преступления является материальным, остается нерешенным вопрос о форме вины в отношении наступивших последствий. Ни в теории, ни в судебной практике нет однозначного решения по разграничению субъективной стороны применительно к деянию и наступившим последствиям.

Одним из вариантов решения данной проблемы является предложение об исключении из состава преступления деяния в виде неправомерного доступа. Таким образом, деянием будет признаваться неправомерное блокирование, модификация, уничтожение компьютерной информации. В данном случае состав будет являться формальным, а форма вины будет выражаться исключительно в виде прямого умысла, что свойственно сущности таких деяний как преступных.

8) В настоящее время п. 3 ст. 272 УК РФ объединяет в себе оба признака, а именно совершение преступления группой лиц по предварительному сговору и организованной группой.

По нашему мнению, совмещение в одном пункте статьи различных по общественной опасности обстоятельств является законодательным несовершенством. Так, в Уголовном кодексе такие признаки состава как совершение преступления группой лиц по предварительному сговору и организованной группой соотносятся в различных главах как

квалифицирующий и особо квалифицирующий признак. Нами представляется возможным выделить данные признаки в разные пункты статьи и усилить ответственность за совершение неправомерного доступа к компьютерной информации, совершенного организованной группой, поскольку совершение деяния в составе организованной группы несет в себе большую общественную опасность, нежели совершение неправомерного доступа группой лиц по предварительному сговору.

9) Частью 4 ст. 272 УК РФ предусмотрена ответственность за деяния предусмотренные частями первой, второй или третьей, если они повлекли тяжкие последствия или создали угрозу их наступления.

Понятие «тяжкие последствия» в диспозиции статьи не раскрывается, является оценочным и определяется судом в каждом конкретном случае в зависимости от обстоятельств дела.

В «Методических рекомендациях по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации», приводятся примеры тяжких последствий применительно к статье 273 УК РФ. Однако данный акт не раскрывает того, что понимать под тяжкими последствиями применительно к ч. 4 ст. 272 УК РФ.

По нашему мнению, применять аналогию в данном случае нельзя, поскольку не все из указанных в Методических рекомендациях тяжкие последствия будут полностью охватываться ч. 4 ст. 272 УК РФ.

Причинение тяжкого вреда здоровью, смерти, а также иные наступившие последствия, являющиеся преступлениями, предусмотренными статьями УК РФ, санкция за которые строже, чем предусмотренная за составное преступление, не может охватываться частью 4 ст. 272 УК РФ и такие последствия должны быть квалифицированы по совокупности.

В случае, когда особо крупный материальный ущерб причиняется преступлением, объектом которого выступает собственность (такие как мошенничество или кража) такие действия также должны квалифицироваться по совокупности.

10) Кроме того, нами был рассмотрен вопрос об отграничении неправомерного доступа к компьютерной информации от иных видов преступных посягательств, связанных с уничтожением, блокированием, модификацией либо копированием информации, преступлений, предметом которых является компьютерная информация.

Прежде всего, необходимо разграничивать преступления, предусмотренные статьями 273, 274, 274.1 УК РФ, которые расположены в главе 28 УК РФ – преступления в сфере компьютерной информации. Родовым объектом, таких преступлений, как и в ст. 272 УК РФ, будут признаваться общественные отношения, обеспечивающие общественную безопасность и общественный порядок.

Преступления, предусмотренные ст. 272 УК РФ и 273 УК РФ, различаются по таким признакам как предмет, объективная сторона и субъективная сторона, и должны быть квалифицированы по правилам совокупности, в случае, когда деяние содержит признаки данных преступлений.

Смежными составами являются ст. 272 УК РФ и ст. 274 УК РФ. Объективная сторона преступлений различна, в связи с чем, квалификация таких деяний по совокупности исключена. Так, указанные в законе последствия наступают вследствие совершения различных деяний. Применению подлежит только одна норма.

По правилам квалификации общей и специальной норм должны разрешаться случаи, когда применению подлежит ч. 1 ст. 272 УК РФ и ч. 2 ст. 274.1 УК РФ, где ч. 1 ст. 272 УК РФ является общей, а ч. 2 ст. 274.1 УК РФ специальной. Так, ч. 2 ст. 274.1 УК РФ предусматривает ответственность за аналогичные деяния в отношении специального предмета – информации, содержащейся в критической информационной инфраструктуре.

Преступления, предусмотренные ст. 272 УК РФ и ст. 159.6 УК РФ (мошенничество в сфере компьютерной информации) должны быть квалифицированы по правилам совокупности преступлении, в том случае, если деяние содержит признаки этих преступлений.

Квалификация по совокупности преступлений в данном случае является правильной, поскольку, во-первых, признак неправомерности доступа к охраняемой законом компьютерной информации статьей 159.6 УК РФ не предусмотрен, а во-вторых, статья 159.6 УК РФ не предусматривает более строгое наказание за совершение мошенничества в сфере компьютерной информации, а, следовательно, принцип справедливости, согласно которому не допускается двойная ответственность за одно деяние, не нарушается.

Кроме того, по правилам совокупности должно быть квалифицировано каждое из следующих деяний, совершаемых путем неправомерного доступа к компьютерной информации (то есть такие деяния, последствием которых является уничтожение, блокирование, модификация либо копирование компьютерной информации, и, предметом которых является компьютерная информация): ст. 138 УК РФ (Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений); ст. 146 УК РФ (Нарушение авторских и смежных прав); ст. 147 УК РФ (Нарушение изобретательских и патентных прав); ст. 183 УК РФ (Незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну); ст. 283.1 (Незаконное получение сведений, составляющих государственную тайну) и другие.

Таким образом, нами были выявлены проблемные моменты применения указанной нормы. По нашему мнению, предложенные изменения статьи, предусматривающей ответственность за неправомерный доступ к компьютерной информации, способны повлечь за собой разрешение ряда проблем, возникающих в правоприменении.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Нормативно-правовые акты.

1. Европейская конвенция по киберпреступлениям от 21.11.2001. [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». Режим доступа: http://www.consultant.ru.

2. Соглашения о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 1 июня 2001 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

3. Уголовный кодекс Российской Федерации. [Электронный ресурс] : федер. закон от 13.06.1996 № 63-ФЗ ред. от 12.04.2020 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

4. О безопасности [Электронный ресурс] : федер. закон от 28.12.2010 № 390-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

5. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс] : федер. закон от 07.12.2011 № 420-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

6. О коммерческой тайне [Электронный ресурс] : федер. закон от 29.07.2004 № 98-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

7. О персональных данных [Электронный ресурс] : федер. закон от 27.07.2006 № 152-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

8. О связи [Электронный ресурс] : федер. закон от 07.07.2003 № 126-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

9. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : федер. закон от 27.07.2006 № 149-ФЗ // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

10. Об утверждении Перечня сведений конфиденциального характера [Электронный ресурс] : Указ Президента РФ от 06.03.1997 № 188 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

11. Методические рекомендации по осуществлению прокурорского надзора за исполнением законов при расследовании преступлений в сфере компьютерной информации [Электронный ресурс] : утв. Генпрокуратурой России от 30.05.2014 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

12. На проект Федерального закона «О внесении изменений в Уголовный кодекс Российской Федерации и отдельные акты Российской Федерации» [Электронный ресурс] : Официальный отзыв ВС РФ от 7.04.2011 г. № 1/общ-1583 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

13. На проект Федерального закона № 559740-5 «О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ» (к первому чтению) [Электронный ресурс] : Заключение Комитета Государственной Думы по информационной политике, информационным технологиям и связи от 05.07.2011 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

14. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения – М: Стандартинформ, 2009.

2. Специальная литература.

15. Абов, А. И. Преступления в сфере компьютерной информации. / Абов Алексей Иванович. – Москва : 2002. – С. 13.

16. Айсанов, Р. М. Состав неправомерного доступа к компьютерной информации, в Российском, международном и зарубежном уголовном законодательстве . : автореф. дис. …. канд. юр. наук : 12.00.08 / Айсанов Руслан Мухамедович. – Москва, 2006. – 31 с.

17. Алескеров, В.И. Уголовно-правовая и криминалистическая характеристика современных видов преступлений в сфере компьютерной информации: Лекция. [Электронный ресурс] / Алескеров В.И., Максименко И.А. –Домодедово: ВИПК МВД России, 2011. – Режим доступа: http://www.elibrary.ru.

18. Болсуновская, Л.М. Анализ способов совершения мошенничества в сфере компьютерной информации [Электронный ресурс] / Л. М. Болсуновская // Проблемы экономики и юридической практики. – 2015. – № 2. – Режим доступа: http://www.consultant.ru.

19. Волеводз, А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества [Электронный ресурс] : монография / А. Г. Волеводз. – Москва: Юрлитинформ, 2011. – Режим доступа: http:// www.mgimo.ru.

20. Гавло, В.К. Некоторые особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации [Электронный ресурс] / В.К. Гавло, В.В. Поляков // Известия государственного Алтайского университета. – 2006. – № 2. – Режим доступа: http://www.consultant.ru.

21. Гаврилин, Ю.В. Расследование неправомерного доступа к компьютерной информации [Электронный ресурс] : учеб. пособие: / под ред. Н.Г. Шурухнова. Москва : ЮИ МВД РФ; Книжный мир, 2001. – Режим доступа: http://www. law.edu.ru.

22. Гребеньков, А. А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава [Электронный ресурс] / А. А. Гребеньков // Lex russica – 2018. – № 4. – Режим доступа: http://www.consultant.ru.

23. Дремлюга, Р. И. Компьютерная информация как предмет преступления, предусмотренного ст. 272 УК РФ [Электронный ресурс] / Р. И. Дремлюга // Уголовное право. – 2018. – № 4. – Режим доступа: http://www.consultant.ru.

24. Евдокимов, К. Н. Некоторые особенности уголовно-правовой квалификации неправомерного доступа к компьютерной информации на стадии возбуждения уголовного дела [Электронный ресурс] / К. Н. Евдокимов – Российский следователь. – 2017. – № 4. – Режим доступа: http://www.consultant.ru.

25. Елин, В. М. Мошенничество в сфере компьютерной информации как новый состав преступления [Электронный ресурс] / В. М. Елин // Бизнес-информатика. – 2013. – № 2. – Режим доступа: http://cyberleninka.ru.

26. Ефремова, А. М. К вопросу о понятии компьютерной информации [Электронный ресурс] / А. М. Ефремова // Юрист. – 2012. – № 1. – Режим доступа: http://www.consultant.ru.

27. Ефремова, Т. Ф. Новый словарь русского языка. Толково-образовательный: в 2х т. / Т. Ф. Ефремова – Москва : Русс. Яз., 2000.– Т. 1. – С. 1209.

28. Зинина, У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве [Электронный ресурс] : Дис. ... канд. юрид. наук. : 12.00.08 / Зинина Ульяна Викторовна. – Москва , 2007. – Режим доступа: http://www.diss.seluk.ru.

29. Зубова, М. А. Неправомерный доступ к компьютерной информации и его последствия [Электронный ресурс] / М. А. Зубова // Бизнес в законе. Экономико-юридический журнал. – 2007. – № 3. – Режим доступа: http://www.cyberleninka.ru.

30. Иногамова-Хегай, Л.В Концептуальные основы конкуренции уголовно-правовых норм [Электронный ресурс] : монография / Л.В. Иногамова-Хегай – Москва : Норма, Инфра-М, 2015. – Режим доступа: http://www.consultant.ru.

31. Кабанова, А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты) : автореф. дис. ... канд. юрид. наук. 12.00.08 / Кабанова Анна Жунусовна. – Ростов-на-Дону, 2004. – 28 с.

32. Карпов, В.С. Уголовная ответственность за преступления в сфере компьютерной информации : дис….канд. юридических наук : 12.00.08 / Карпов Виктор Сергеевич – Красноярск, 2002. – 134 с.

33. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [Электронный ресурс] / под ред. А. В. Бриллиантова. – Режим доступа: http://www.consultant.ru.

34. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / [Электронный ресурс] / под ред. В. М. Лебедева. – Режим доступа: http://www.consultant.ru.

35. Куприянов, А.И. Оптимизация мер по защите с учетом ценности информации [Электронный ресурс] / А.И. Куприянов, В.В. Шевцов – М.: Известия института инженерной физики. – 2012. – № 25. – Режим доступа: http://www.elibrary.ru.

36. Крылов, В. В. Информационное копирование преступления / В.В. Крылов – М., 1997. – С. 67.

37. Малыковцев, М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ : дисс … канд. юр. наук : 12.00.08 / Малыковцев Михаил Михайлович. – М., 2006. – С. 108.

38. Малышенко, Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации : дисс …. канд. юр. наук. : 12.00.08 / Малышенко Дмитрий Геннадьевич. – М., 2009. – С. 56.

39. Мицкевич, А. Ф. Понятие компьютерной информации по российскому и зарубежному уголовному праву [Электронный ресурс] / А. Ф.Мицкевич, А. В. Суслопаров // Пробелы в российском законодательстве. Юридический журнал. – 2010. – № 2. – Режим доступа: http://www.cyberleninka.ru.

40. Нагорный, А.А. Содержание понятия «компьютерная информация» как предмета компьютерных преступлений [Электронный ресурс] / А.А. Нагорный // Актуальные проблемы российского права. – 2014. – № 1. – Режим доступа: http://www.consultant.ru.

41. Никифоров, Б. С. Объект преступления по советскому уголовному праву [Электронный ресурс] / Б. С. Никифоров // Правоведение. –1962. – № 1. – Режим доступа: http://www. law.edu.ru.

42. Новое в Уголовном кодексе (постатейный) [Электронный ресурс] / под ред. А. И. Чучаева. – Режим доступа: http://www.consultant.ru.

43. Об авторском праве и смежных правах [Электронный ресурс] : закон ФРГ// Адвокатская канцелярия. – Режим доступа: http://www.advokat-engelmann.de.

44. Питецкий, В. В. Копирование как последствие неправомерного доступа к компьютерной информации. В.В. Питецкий, А.О. Надводнюк // Сибирский антропологический журнал. – 2019. – № 2 (6). – С. 38-43.

45. Полубинская, С. В. Учебный комментарий к уголовному кодексу Российской Федерации / под ред. М. Жалинского – Москва : Эксмо, 2005. – С. 837.

46. Решетников, А.Ю. Некоторые вопросы квалификации неоконченных преступлений в сфере компьютерной информации [Электронный ресурс] / А.Ю. Решетников, Е.А. Русскевич // Уголовное право. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

47. Решетников, А. Ю. Об уголовной ответственности за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК России) [Электронный ресурс] / А. Ю.

Решетников, Е.А. Русскевич // Законы России: опыт, анализ, практика. – 2018. – № 2. – Режим доступа: http://www.consultant.ru.

48. Степанов-Егиянц, В. Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации [Электронный ресурс] : монография / В. Г. Степанов-Егиянц. – М.: Статут, 2016. – Режим доступа: http://www.consultant.ru.

49. Степанов-Егиянц, В. Г. Содержание термина «неправомерный доступ» в Уголовном кодексе РФ [Электронный ресурс] / В. Г. Степанов-Егиянц // Право и экономика. – 2014. – № 8. – Режим доступа: http://www.consultant.ru.

50. Степанов-Егиянц, В. Г. Характеристика субъекта неправомерного доступа к компьютерной информации по Уголовному кодексу РФ [Электронный ресурс] / В. Г. Степанов-Егиянц // Законодательство. – 2014. – № 7. – Режим доступа: https://base.garant.ru.

51. Суслопаров, А. В. Информационные преступления : автореф. дис….канд. юридических наук : 12.00.08 / Суслопаров Алексей Валерьевич – Красноярск, 2008. – 24 с.

52. Суслопаров, А. В. Компьютерные преступления как разновидность преступлений информационного характера. : дис. …. канд. юр. наук : 12.00.08 / Суслопаров Алексей Валерьевич. – Красноярск, 2010. – 206 с.

53. Тарбагаев, А. Н. Ответственность за неправомерный доступ к компьютерной информации: уголовно-правовой и административно-правовой аспект [Электронный ресурс] / А. Н. Тарбагаев, А. В. Суслопаров // Вестник Омского университета. – 2012. – № 2. – Режим доступа: http://www.cyberleninka.ru.

54. Третьяк, М. И. Модификация компьютерной информации и ее соотношение с другими способами компьютерного мошенничества [Электронный ресурс] / М. И. Третьяк // Уголовное право. – 2016. – № 2. – Режим доступа: http://www.consultant.ru.

55. Уголовное право. Особенная часть : учебник / под ред. Л.В. Иногамовой-Хегай. – 2-е изд., с изм и доп. – Москва : Инфра-М, 2008. – С. 467.

56. Уголовное право. Общая часть : учебник / под ред. И. Я. Козаченко. – Москва : Норма, 2008. – 720 с.

57. Уголовное право. Общая часть : учебник / под ред. А. И. Рарога. – 3-е изд., с изм и доп. – Москва : Эксмо, 2009. – 438 с.

58. Уголовное право. Общая часть : учебник / под ред. А. Н. Тарбагаева. – Москва : Проспект, 2011. – 448 с.

59. Уголовное право. Особенная часть : учебник / под ред. И. В. Шишко. – Москва : Проспект, 2011. – 752 с.

60. Уголовный кодекс КНР [Электронный ресурс] // Посольство Китайской Народной Республики в Российской Федерации. – Режим доступа: http://ru.china-embassy.org.

61. Уголовный кодекс ФРГ [Электронный ресурс] // Российский правовой портал: библиотека Пашкова. – Режим доступа: http://www.constitutions.ru.

62. Фатьянов, А. А. О дефиниции «компьютерная информация» в российском уголовном законодательстве [Электронный ресурс] / А. А. Фатьянов // Информационное право. – 2017. – № 3. – Режим доступа: http://www.cyberleninka.ru.

63. Халлиулин, А. И. Неправомерное копирование как последствие преступлений в сфере компьютерной информации [Электронный ресурс] / А. И. Халлиулин // Российский следователь. – 2015. – № 8. – Режим доступа: http://www.consultant.ru.

64. Хлупина, Г. Н. Квалификация нескольких преступлений : учебное пособие / Г. Н. Хлупина. – Красноярск : ИПК СФУ, 2009. – 74 с.

65. Шевелева, С. В. Мошенничество в сфере компьютерной информации: особенности квалификации и конкуренции со смежными составами [Электронный ресурс] / С. В. Шевелева // Юридическая наука и

практика: Вестник Нижегородской академии МВД России. – 2017. – № 4. – Режим доступа: http://cyberleninka.ru.

3. Судебная практика.

66. О судебной практике по делам о краже, грабеже и разбое [Электронный ресурс] : Постановлению пленума Верховного Суда РФ от 27.12.2002 № 29 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

67. О судебной практике по делам о мошенничестве, присвоении и растрате [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 30 ноября 2017 г. № 48 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

68. О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 16 октября 2009 г. № 19 // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

69. О некоторых вопросах судебной практики по делам о преступлениях против конституционных прав и свобод человека и гражданина (статьи 137, 138, 138.1, 139, 144.1, 145, 145.1 Уголовного кодекса Российской Федерации) [Электронный ресурс] : Постановление Пленума Верховного Суда РФ от 25 декабря 2018 г. № 46. // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

70. Постановление Президиума Самарского областного суда от 14 февраля 2019 г. № 44у-36,37/2019 [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

71. Апелляционным постановлением Московского городского суда от 15 июня 2016 г. по делу № 10-7792/16 [Электронный ресурс] // Справочная

правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

72. Справка Верховного Суда Республики Крым по результатам изучения судебной практики по уголовным делам о преступлениях в сфере компьютерной информации (гл. 28 УК РФ) [Электронный ресурс] // Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

73. Приговор Белгородского районного суда Белгородской области от 16 сентября 2010 г. по делу № 1-43/2010 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

74. Приговор Промышленного районного суда г.Оренбурга от 27.02.2011 № 1-55/2011 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

75. Приговор Перовского районного суда города Москвы от 10.10.2014 по делу № 1-975/2014 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

76. Приговор Кировоградского городского суда Свердловской области от 05.08.2016 по делу № 1-105/2016 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.rospravosudie.com.

77. Приговор Кировского районного суда г. Хабаровска (Хабаровский край) № 1-3/2017 1-45/2016 от 23 марта 2017 г. по делу № 1-3/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

78. Приговор Ленинского районного суда г. Владикавказа № 1-356/2017 1-44/2018 от 14 февраля 2018 г. по делу № 1-356/2017 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

79. Приговор Советского районного суда г. Казани № 1-212/2018 от 15.05. 2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

80. Приговор Золотухинского районного суда Курской области № 1-28/2018 от 23 мая 2018 г. по делу № 1-28/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

81. Приговор Зареченского районного суда г.Тулы от 04.06.2018 № 1-41/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

82. Приговор Канавинского районного суда г.Нижний Новгород от 06.06.2018 № 1-283/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

83. Приговор Кировского районного суда г.Астрахани от 13.06.2018 № 1-250/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

84. Приговор Ленинского районного суда г. Владимира № 1-211/2018 от 27 июля 2018 г. по делу № 1-211/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

85. Приговор Советского районного суда г. Томска от 08.02.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

86. Приговор Балтийского городского суда № 1-12/2019 от 19.02.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

87. Приговор Центрального районного суда г. Читы № 1-54/2019 1-950/2018 от 20 февраля 2019 г. по делу № 1-54/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

88. Приговор Мотовилихинского районного суда г. Перми от 25.02.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

89. Приговор Ленинского суда г.Тамбова № 1-60/2019 от 21 марта 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

90. Приговор Энгельского районного суда № 1-1-203/2019 1-203/2019 от 21.03.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

91. Приговор Егорьевского городского суда Московской области от 15.04.2019 № 1-220/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

92. Приговор Октябрьского районного суда г. Ростова-на-Дону от 22.04.2019 № 1-306/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

93. Приговор Советского районного суда г. Орла № 1-43/2019 от 13 июня 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

94. Приговор Центрального районного суда г. Челябинска № 1-297/2019 от 17 июня 2019 г. по делу № 1-297/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

95. Приговор Октябрьского районного суда г. Красноярска № 1-346/2019 от 8 июля 2019 г. по делу № 1-346/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

96. Приговором Ленинского районного суда г. Пензы № 1-145/2019 от 17 июля 2019 г. по делу № 1-145/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

97. Приговор Мариинско-Посадский районный суд Чувашской республики № 1-54/2019 от 26 июля 2019 г. по делу № 1-54/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

98. Приговор Якутского городского суда № 1-681/2019 от 26 августа 2019 г. по делу № 1-1462/2018 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

99. Приговор Ленинградского районного суда Краснодарского края № 1-110/2019 от 27 августа 2019 г. по делу № 1-110/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

100. Приговор Кирсановского районного суда (Тамбовской области) № 1-140/2019 от 28 августа 2019 г. по делу № 1-140/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

101. Приговор Лысковского районного суда Нижегородской области от 02.11.2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

102. Приговор Ленинского суда г.Тамбова № 1-60/2019 от 21 марта 2019 г. [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

103. Приговор Егорьевского городского суда Московской области от 15.04.2019 № 1-220/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

104. Приговор Октябрьского районного суда г. Ростова-на-Дону от 22.04.2019 № 1-306/2019 [Электронный ресурс] // Судебные и нормативные акты РФ. – Режим доступа: http://www.sudact.ru.

4. Электронные ресурсы.

105. Адвокатская канцелярия. – Режим доступа: http://www.advokat-engelmann.de.

106. Бесплатная электронная библиотека – Режим доступа: http://www.diss.seluk.ru.

107. Научная электронная библиотека «elibrary» – Режим доступа: http://www.elibrary.ru.

108. Научная электронная библиотека «КИБЕРЛЕНИНКА». – Режим доступа: http://www.cyberleninka.ru.

109. Официальный сайт МГИМО – Режим доступа: http:// www.mgimo.ru.

110. Посольство Китайской Народной Республики в Российской Федерации. – Режим доступа: http://ru.china-embassy.org.

111. Правовой портал «Юридическая Россия» – Режим доступа: http://www. law.edu.ru.

112. Российский правовой портал: библиотека Пашкова. – Режим доступа: http://www.constitutions.ru.

113. «РосПравосудие» – судебная практика – Режим доступа: http://www.rospravosudie.com.

114. Справочная правовая система «КонсультантПлюс». – Режим доступа: http://www.consultant.ru.

115. СудАкт – судебные и нормативные акты РФ – Режим доступа: http://www.consultant.ru.

116. Электронная библиотека – Режим доступа: https://www.twirpx.com.

Федеральное государственное автономное
образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Юридический институт
Кафедра уголовного права

УТВЕРЖДАЮ
Заведующий кафедрой
_____ А. Н. Тарбагаев
подпись инициалы, фамилия
«28» 05 _____ 2020 г.

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

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

40.04.01 – Юриспруденция
код и наименование направления

40.04.01.01 – Правосудие по уголовным делам
код и наименование магистерской программы

Научный руководитель 28.05.2020 доцент, к.ю.н. В.В. Питецкий
подпись, дата должность, ученая степень инициалы, фамилия

Выпускник 28.05.2020 А.О. Надводнюк
подпись, дата инициалы, фамилия

Рецензент 28.05.20 прокурор Манского района, старший советник юстиции С.Н. Коряков
подпись, дата должность, звание инициалы, фамилия

Красноярск 2020