МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт права
(наименование института полностью)

Кафедра «Уголовное право и процесс»
(наименование)

40.03.01 Юриспруденция
(код и наименование направлению подготовки / специальности)

Уголовно-правовой
(направленность (профиль) / специализация)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

на тему «Уголовная ответственность за преступления в сфере компьютерной информации»

Обучающийся С.В. Кукушкин
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент, А.С. Таран
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2023

Аннотация

Тема выпускной квалификационной работы: Уголовная ответственность за преступления в сфере компьютерной информации.

Целью исследования является выявление особенностей уголовно-правового регулирования и практики привлечения к ответственности за совершение преступлений в сфере компьютерной информации, а также формирование предложений по совершенствованию данной сферы правоотношений.

Для достижения данной цели были поставлены следующие задачи:

- рассмотреть понятие и законодательное регулирование использования компьютерной информации;
- раскрыть понятие, систему и общую характеристику преступлений в сфере компьютерной информации по российскому уголовному законодательству;
- проанализировать объективные и субъективные признаки основных составов преступлений, предусмотренных ст. 272-274.2 УК РФ;
- охарактеризовать квалифицирующие признаки преступлений в сфере компьютерной информации;
- выявить особенности квалификации преступлений в сфере компьютерной информации (на основе анализа материалов судебной практики);
- обозначить направления совершенствования уголовной ответственности за преступления в сфере компьютерной информации.

Работа состоит из введения, трех глав, объединяющих шесть параграфов, заключения, списка используемой литературы и используемых источников.

Оглавление

Введение

Актуальность темы исследования. С увеличением использования компьютерных технологий и интернета во всех сферах жизнедеятельности, преступления, связанные с неправомерным оборотом компьютерной информации, становятся все более распространенными во всем мире. Это может включать в себя различные виды киберпреступлений, такие как хакерство, фишинг, мошенничество с использованием платежных систем и другие формы компьютерной преступности.

Причины роста таких преступлений могут быть связаны с развитием научно-технического прогресса, который создает новые возможности и инструменты для киберпреступников. Быстрый рост числа людей, использующих электронные средства платежа и приложения, работающие через интернет, также создает больше возможностей для совершения преступлений в сети.

Для борьбы с киберпреступностью важно принимать меры как на государственном уровне, так и на уровне отдельных организаций и отдельных лиц. Государства должны разрабатывать и усовершенствовать законы, регулирующие киберпреступность, и создавать специализированные органы для расследования и пресечения таких преступлений.

С развитием мобильных устройств и приложений, появляются новые виды киберпреступлений, связанных с мобильной сферой. Например, вредоносные программы, разработанные специально для атак на мобильные устройства, мошенничество с использованием мобильных платежных систем и фишинг через мобильные приложения. Преступники также могут использовать мобильные устройства для хранения и распространения незаконного контента, такого как детская порнография или наркотики.

Развитие компьютерных технологий и распространение их использования на планшетах, смартфонах и других устройствах приводит к тому, что преступники находят новые способы использования этих

технологий в своих криминальных действиях. Это создает новые вызовы для правоохранительных органов и общества в целом, и связано с необходимостью адаптации законодательства к новым вызовам и угрозам, связанным с компьютерной информацией и информационными технологиями.

В России действующий Уголовный кодекс Российской Федерации устанавливает ответственность за преступления в сфере компьютерной информации в главе 28 (далее - УК РФ [58]). Цель данной главы Уголовного кодекса состоит в защите информационных ресурсов, безопасности данных и обеспечении прав граждан на конфиденциальность и неприкосновенность информации. Она предусматривает установление наказания для лиц, совершающих преступления в сфере компьютерной информации, с целью предотвращения и пресечения таких противоправных действий.

При этом, при квалификации преступлений в сфере компьютерной информации возникают различные проблемы, которые связаны как с определением признаков составов этих преступлений, так и с их отграничением от смежных деяний. Эти проблемы могут быть вызваны быстрым развитием технологий и появлением новых видов киберпреступлений, а также различиями в интерпретации законодательства и судебной практики.

Определение признаков составов преступлений в сфере компьютерной информации может быть сложным из-за технической сложности и специфики таких преступлений. Киберпреступления могут быть масштабными и международными, вовлекать различные виды технических и программных средств, а также иметь новые формы и методы совершения. Это создает трудности при определении конкретных признаков преступления и его квалификации.

Кроме того, отграничение преступлений в сфере компьютерной информации от смежных деяний также может быть проблематичным. Например, определение границы между киберпреступлениями и обычным мошенничеством может быть сложным, особенно когда мошеннические

действия совершаются с использованием компьютерных технологий. Также возникают вопросы относительно отличия между хакерскими атаками и исследовательскими действиями в области кибербезопасности.

Исследователи, правоохранительные органы и юристы ведут дискуссии и проводят исследования по рассматриваемым вопросам, однако до настоящего времени единого мнения по многим аспектам квалификации преступлений в сфере компьютерной информации нет. Разнообразие судебной практики и различные подходы к квалификации могут привести к неоднозначным решениям в конкретных случаях. Все это определяет актуальность темы настоящего исследования.

Состояние научной разработанности темы. Вопросы данной проблематики в той или иной степени освещены в работах таких исследователей, как Ю.В. Белевитина, И.А. Белоус, С.Д. Бражник, В.Н. Винокуров, Е.Е. Гурьева, А.С. Джилкашиев, И.Н. Крапчатова, М.И. Лавицкая, Ю.А. Левашов, А.Н. Лыженкова, А.С. Матиенко, А.В. Мнацаканян, В.М. Пестриков, Г.А. Петров, А.А. Фатьянов, Д.А. Чудов, Е.А. Шматко, и др. Они составили основу нашего исследования, отразив, прежде всего - структуру анализируемой темы и наиболее важные ее вопросы.

Целью исследования является выявление особенностей уголовно-правового регулирования и практики привлечения к ответственности за совершение преступлений в сфере компьютерной информации, а также формирование предложений по совершенствованию данной сферы правоотношений.

Для достижения данной цели были поставлены следующие задачи:

- рассмотреть понятие и законодательное регулирование использования компьютерной информации;
- раскрыть понятие, систему и общую характеристику преступлений в сфере компьютерной информации по российскому уголовному законодательству;

- проанализировать объективные и субъективные признаки основных составов преступлений, предусмотренных ст.ст. 272-274.2 УК РФ;
- охарактеризовать квалифицирующие признаки преступлений в сфере компьютерной информации;
- выявить особенности квалификации преступлений в сфере компьютерной информации (на основе анализа материалов судебной практики);
- обозначить направления совершенствования уголовной ответственности за преступления в сфере компьютерной информации.

Объектом настоящего исследования являются отношения, возникающие в сфере квалификации преступлений в сфере компьютерной информации.

Предметом исследования выступают уголовно-правовые нормы, предусматривающие ответственность за совершение преступлений в сфере компьютерной информации, научные труды по данному вопросу и материалы правоприменительной практики.

Практическая значимость исследования заключается в возможности применения его теоретических выводов, предложений и рекомендаций в повышении эффективности правоприменительной деятельности, связанной с квалификацией преступлений в сфере компьютерной информации.

Методологическая основа исследования. Методологическую основу исследования составляет система общефилософских, общенаучных и специально-научных методов, обеспечивающих объективный анализ исследуемого предмета. С учетом специфики, темы, цели и задач исследования автор использовал следующие методы:

- диалектический метод познания (дает возможность исследовать природу и сущность уголовной ответственности за совершение компьютерных преступлений);

- структурно-функциональный и формально-юридический методы (использован автором при анализе структуры уголовной ответственности за совершение компьютерных преступлений);
- сравнительно-правовой метод (его применение дает возможность определить общие и специфические признаки понятий уголовной ответственности);
- социологический метод (дает возможность исследовать проблемы уголовной ответственности в теоретическом аспекте).

Методологическую основу исследования составляют диалектический материализм как всеобщий метод познания, а также частно-научные методы: системный, логический, статистический, конкретно-социологический, анализ, синтез и другие.

Концепция уголовно-правового регулирования и практики привлечения к ответственности за преступления в сфере компьютерной информации в настоящее время находится в стадии формирования, поэтому в исследовании крайне важна роль институционального подхода. С его помощью возможно изучить функции современных институциональных изменений изучаемого правового института.

Формально-юридический метод применен в целях анализа нормативных предписаний, а также в определении проблем правового регулирования и поиске путей совершенствования данной сферы правоотношений.

Эмпирическая база исследования представлена постановлениями и определениями высших судебных органов, материалами опубликованной судебной практики, а также эмпирическими материалами научно-практических конференций и статистическими данными.

Структура работы определена задачами и логикой проведенного исследования, включает в себя введение, три главы, состоящие из шести параграфов, заключения и списка используемой литературы и используемых источников.

Глава 1 Уголовно-правовая политика в сфере охраны компьютерной информации в Российской Федерации

1.1 Понятие и законодательное регулирование использования компьютерной информации

В настоящее время киберпреступления представляют огромную проблему для мирового сообщества, т.к. в современном обществе киберпреступность является, на наш взгляд, основной угрозой не только национальной безопасности, но и всему мировому сообществу.

Компьютерная информация выступает предметом преступлений, предусмотренных главой 28 УК РФ. Федеральным законом от 07.12.2011 № 420-ФЗ были внесены изменения в Уголовный кодекс Российской Федерации, в том числе в главу 28, которая регулирует преступления в сфере информационных технологий [25]. Одним из основных изменений была новая формулировка понятия «компьютерная информация», которая учтена в новой редакции статьи 272 УК РФ.

Преступления, связанные с компьютерной информацией, теперь могут включать в себя любые действия, связанные с электрическими сигналами, независимо от конкретного средства их хранения, обработки или передачи [28]. Примерами таких преступлений могут быть незаконный доступ к компьютерной информации, создание и распространение вредоносных программ, мошенничество с использованием компьютерной информации и т.д. Эти изменения были внесены для обеспечения более широкого понимания и учета современных технологических реалий в сфере информационной безопасности и борьбы с компьютерными преступлениями.

Активное внедрение информационных технологий привело к развитию цифровых электронных устройств, таких как смартфоны, идентификационные карты с микроконтроллером и «умная» бытовая техника, включая устройства, связанные с концепцией «Интернета вещей». Эти устройства стали широко

распространены и часто используются людьми в повседневной жизни. Такое разнообразие цифровых устройств и их влияние на обработку информации привели к тому, что персональный компьютер уже не рассматривается единственным инструментом для работы с цифровой информацией. Поэтому предыдущее устаревшее определение компьютерной информации, ограниченное персональным компьютером, стало неприменимым и сужало рамки применения уголовного закона в сфере информационных преступлений.

Целесообразна классификация электронных носителей информации следующим образом:

- по характеру связи с расследуемым событием: первичные, вторичные;
- по форме представления информации: письменные, электронные (включая электронные документы, электронную переписку, электронные базы данных и другие формы электронных записей), аудио- и видеозаписи;
- по способу получения информации: изъятые непосредственно у подозреваемого или других лиц, полученные от третьих лиц по запросу, полученные путем технических мероприятий (например, с использованием программного обеспечения для извлечения информации с жесткого диска или мобильного устройства);
- по источнику информации: смартфоны, компьютеры, серверы, облачные хранилища, носители информации (например, USB-накопители, внешние жесткие диски, CD/DVD-диски);
- по статусу информации: открытая (содержимое носителя доступно без применения специальных технических средств), зашифрованная (содержимое носителя защищено паролем или шифрованием);
- по временному периоду: текущие (содержащие информацию, актуальную на момент изъятия) и архивные (содержащие информацию, накопленную в прошлом и имеющую историческую

ценность).

- по возможности перемещения в пространстве: стационарные, портативные; Стационарные информационные системы представляют собой компьютерные системы или другие устройства, которые не предназначены для перемещения информации из одной системы в другую. Они обычно фиксируются в определенном месте, таком как офис или серверная комната, и предназначены для обработки и хранения информации на месте. Примерами стационарных информационных систем могут служить рабочие станции, серверы или специализированные компьютерные системы, используемые в определенных отраслях.

Портативные информационные системы могут быть мобильными устройствами, такими как ноутбуки, планшеты, смартфоны или переносные жесткие диски. Портативные системы позволяют пользователям работать с информацией в разных местах и обмениваться ею с другими системами или пользователями. Такие системы обычно имеют встроенные средства беспроводной связи, такие как Wi-Fi или Bluetooth, чтобы обеспечить подключение к другим системам или сетям.

По типу устройства хранения информации: внутренние и внешние.

Внутренние устройства хранения информации обычно встроены непосредственно в компоненты системы, такие как жесткие диски (HDD) или твердотельные накопители (SSD) внутри компьютера или сервера. Внутренние устройства хранения обеспечивают быстрый доступ к данным и обрабатывают больший объем информации. Они предоставляют постоянное и надежное хранение данных, которые используются в рамках конкретной информационной системы.

Внешние устройства хранения информации обычно подключаются к системе через внешние порты, такие как USB, Thunderbolt или сетевые интерфейсы. Примерами внешних устройств хранения информации могут служить внешние жесткие диски, флеш-накопители, сетевые хранилища

(NAS) или облачные сервисы хранения данных. Внешние устройства хранения обеспечивают возможность дополнительного хранения данных, обмена информацией между системами и резервного копирования. Они могут быть переносными и использоваться в различных информационных системах.

Выбор между внутренними и внешними устройствами хранения зависит от конкретных потребностей пользователя или организации. Внутренние устройства обычно предпочтительны для обработки и хранения больших объемов данных в пределах одной информационной системы, в то время как внешние устройства предоставляют гибкость и мобильность для обмена и резервного копирования данных между системами.

По сроку хранения информации: оперативного хранения, временного хранения, постоянного хранения (неограниченно). Оперативное хранение предназначено для хранения информации в течение срока определенного информационного процесса [48, с. 90]. Оно обычно используется для хранения временных данных, которые требуются для выполнения текущих операций и операций обработки данных в режиме реального времени. Примерами оперативного хранения могут служить оперативная память (RAM) компьютера или кэш-память процессора. Оперативное хранение обеспечивает быстрый доступ к данным, но информация в нем обычно не сохраняется после выключения системы или завершения процесса.

Временное хранение предназначено для хранения информации в течение определенного временного интервала. Оно используется для временного хранения данных, которые требуются для обработки, анализа или передачи, но не являются постоянными или долгосрочными. Примерами временного хранения могут служить временные файлы на жестком диске компьютера, кэш-файлы браузера или временные таблицы в базе данных. Временное хранение обычно имеет ограниченный срок хранения, после которого данные могут быть удалены или перезаписаны.

Постоянное хранение предназначено для долгосрочного хранения

информации без ограничений по времени. Оно используется для сохранения данных, которые должны быть доступными и сохраняться в течение продолжительного времени. Примерами постоянного хранения могут служить жесткие диски, сетевые хранилища, оптические диски (например, CD, DVD), магнитные ленты или облачные хранилища данных. Постоянное хранение обеспечивает долгосрочное сохранение информации и защиту от ее случайного удаления или потери.

В зависимости от конкретных требований и политики хранения данных, информационные системы могут использовать комбинацию различных методов хранения для разных типов информации. Например, оперативное хранение может использоваться для временных рабочих данных, временное хранение - для промежуточных результатов, а постоянное хранение - для долгосрочного сохранения важной информации.

Таким образом, классификация электронных носителей информации в уголовно-процессуальном порядке имеет целью систематизацию и организацию доказательственной информации, а также обеспечение ее сохранности и достоверности в ходе расследования преступлений.

Новое определение компьютерной информации, которое учитывает разнообразие цифровых устройств и форму представления информации в виде электрических сигналов, позволяет более точно охватить современные реалии и применять соответствующие нормы уголовного закона к различным видам цифровой информации, независимо от типа устройств, используемых для ее обработки. Это способствует эффективной борьбе с преступлениями, связанными с использованием современных технологий и цифровых устройств.

В современных технологиях передачи и обработки информации доминируют цифровые технологии, где информация представлена в виде дискретных цифровых сигналов. Использование электрических сигналов в таких устройствах и системах является основой для обработки, хранения и передачи информации. Поэтому определение компьютерной информации в

виде электрических сигналов позволяет учесть особенности современных цифровых технологий и широко используемых устройств, основанных на электронных компонентах. Это включает в себя не только персональные компьютеры, но и другие цифровые устройства, такие как смартфоны, идентификационные карты с микроконтроллерами и умная бытовая техника, которые все работают на основе обработки электрических сигналов.

В теории информации указывается, что информация не является просто материальным объектом, а скорее процессом взаимодействия между сознанием человека и внешним стимулом или данными. Информация возникает в результате интерпретации данных человеком. Данные представляют собой сырые факты, символы или наборы символов, которые ещё не имеют осмысленного значения. Они могут быть представлены в различных формах, таких как числа, текст, звуки, изображения и т.д. Однако информация возникает только тогда, когда данные становятся осмысленными и интерпретируются человеком.

Интерпретация данных происходит с участием человеческого сознания, которое присваивает им смысл, связывает их с другими знаниями и контекстом. Таким образом, из одних и тех же данных может быть получена различная информация, в зависимости от контекста, знаний и восприятия человека. Это понимание различия между данными и информацией имеет важное значение, особенно в контексте правовых и уголовных дел, связанных с компьютерной информацией. В правовом контексте, когда речь идет о компьютерной информации как предмете преступлений, уголовное законодательство учитывает, что данные могут быть использованы для различных целей и могут иметь разную интерпретацию и значение для разных сторон, в зависимости от обстоятельств дела и контекста.

В правовом аспекте отметим, что дефиниция компьютерной информации впервые закреплена Федеральным законом от 07.12.2011 № 420-ФЗ [25].

В примечании 1 к ст. 272 УК РФ под компьютерной информацией понимаются «сведения (сообщения, данные), представленные в форме

электрических сигналов, независимо от средств их хранения, обработки и передачи» [57, с. 574].

Сигналы могут быть представлены в различных формах и в разных физических проявлениях, таких как электрические, акустические, магнитные, оптические, механические, световые и другие.

В контексте передачи и обработки информации, электрический сигнал является одной из основных форм сигналов, которые используются в цифровых системах и устройствах. Он описывается физическими величинами, такими как напряжение и ток. В цифровых системах, например, сигналы могут быть представлены в виде бинарных кодов, где электрическое напряжение или ток имеют два уровня, например, «0» и «1».

Электрические сигналы широко используются в электронной и цифровой технике для передачи и обработки информации. Они могут быть сгенерированы и обработаны различными электронными компонентами, такими как транзисторы, интегральные схемы и другие устройства. Электрические сигналы также могут быть преобразованы в другие формы сигналов, например, акустические (звуковые) или оптические (световые), для дальнейшей передачи или восприятия информации.

Верховный Суд РФ разъяснил, что используемый термин «электрический сигнал» в примечании к ст. 272 УК РФ требует дополнительного пояснения.

Проанализировав большое количество правовых документов, мы установили, что прямое определение понятия «компьютерная информация» имеется лишь в Соглашении о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (от 1 июня 2001 г.) - «это информация, находящаяся в памяти компьютера, на машинных или иных носителях в форме, доступной восприятию ЭВМ, или передающаяся по каналам связи» [29]. Соответственно, «используемое понятие «компьютерная», как в названии самой главы 28 УК РФ, так и в тексте статей, входящих в ее состав, на

современном этапе технологического развития общества является неполным» [22, с. 134].

В ранее действовавшем нормативном акте, при определении персональной электронно-вычислительной машины (ЭВМ) - в ГОСТе СССР 15971-90 от 26 октября 1990 года [11], указывалось, что персональная ЭВМ представляет собой стационарный (настольный) компьютер с определенным набором компонентов.

Однако следует отметить, что данное определение устарело и не учитывает современные технологические разработки и разнообразие цифровых устройств, которые сейчас используются для обработки информации. С течением времени технологии электронно-вычислительных устройств претерпели значительные изменения, и теперь понятие персональной ЭВМ уже не ограничивается стационарными компьютерами с указанными компонентами.

Современные цифровые устройства, такие как ноутбуки, смартфоны, планшеты, умные часы и другие, также выполняют функции ЭВМ, позволяя обрабатывать информацию и выполнять различные задачи. Они имеют различные формы и компоненты, но выполняют сходные функции по обработке данных.

Выделяют основные свойства, которыми характеризуется компьютерная информация и которые являются объектами уголовно-правовой охраны: конфиденциальность, целостность и доступность.

Компьютерная информация может содержать конфиденциальные данные, такие как персональные данные, коммерческая информация, банковская информация и т.д. Конфиденциальность информации означает, что доступ к этой информации должен быть ограничен только тем, кому она предназначена, и что она должна быть защищена от неправомерного доступа, использования и раскрытия [6, с. 125].

Целостность информации означает, что информация должна быть защищена от несанкционированного изменения, повреждения или уничтожения.

Это важно для обеспечения достоверности и точности информации, а также для предотвращения фальсификации данных.

Доступность информации означает, что она должна быть доступна и доступна тем, кому она необходима в рамках установленных правил и полномочий [17, с. 25]. Это включает обеспечение доступности информации в случае необходимости, предотвращение несанкционированного блокирования или препятствования доступу к информации

Защита конфиденциальности, целостности и доступности компьютерной информации является важной задачей в сфере информационной безопасности и является объектом уголовно-правовой охраны.

В свете этих свойств, посягательства на целостность, конфиденциальность и доступность информации рассматриваются как общественно-опасные деяния и могут быть квалифицированы как уголовные преступления. Уголовное законодательство обычно предусматривает соответствующие нормы и санкции для защиты информации и наказания лиц, совершающих преступления в отношении такой информации.

1.2 Преступления в сфере компьютерной информации по российскому уголовному законодательству: понятие, система и общая характеристика

Современное общество является информационным, в нем широко представлены информационно-телекоммуникационные (компьютерные) технологии. Более 91 миллиона человек используют мобильный интернет, что говорит о высокой доступности и использовании мобильных устройств для подключения к сети. Зарегистрированные в социальных сетях 53% населения России также указывают на широкое распространение и популярность социальных платформ.

Установлено, что средний россиянин проводит около 6,5 часов в социальных сетях каждый день, что свидетельствует о значительной

активности в сфере онлайн-коммуникаций и обмена информацией в российском обществе. Кроме того, 85% жителей России ежедневно выходят в интернет, что подчеркивает повсеместность и постоянное присутствие информационно-телекоммуникационных технологий в повседневной жизни людей. Это демонстрирует, что Интернет, социальные сети и информационно-телекоммуникационные технологии стали неотъемлемой частью жизни общества в России. Они играют важную роль в коммуникации, обмене информацией, получении новостей, развлечениях, работе, образовании и других сферах деятельности. Однако, с увеличением использования и влияния этих технологий возникают также новые вызовы и задачи, связанные с защитой информации, кибербезопасностью и регулированием в сфере информационных технологий.

Преступления в сфере компьютерной информации - это законодательное определение преступлений, предусмотренных главой 28 УК РФ. «Под преступлением в сфере компьютерной (цифровой) информации следует понимать противоправное виновно совершенное общественно опасное деяние наказуемое в уголовном порядке, посягающее на общественные отношения по безопасному производству, хранению, передаче, поиску, использованию, распространению или защите компьютерной информации, причинившее или создающее угрозу причинения вреда охраняемым законом правам и интересам физических и (или) юридических лиц, общества, государства» [37, с. 59].

Отметим, что законодатель, при конструировании данной главы УК РФ, занимает активную позицию по их совершенствованию.

Так, изначально в главу было включено три состава - это ст. 272-274 УК РФ. В 1994 г. был принят Гражданский кодекс РФ [12], который содержит ряд норм, связанных с компьютерной информацией, а в 1995 г. - Федеральный закон «Об информации, информатизации и защите информации» [31], затем - Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и защите информации» (далее - Закон об информации [32]).

По мнению Солнцева М.Н. «логическим развитием правовой системы, создающей условия безопасности компьютерной информации, стала разработка в УК РФ 1996 года группы статей, предусматривающих основания уголовной ответственности за преступления в сфере компьютерной информации» [51, с. 100].

Позже, с 01 января 2018 года глава 28 УК РФ была дополнена еще одним самостоятельным составом преступления – «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» (ст. 274.1 УК РФ). Данная норма введена законодателем в связи с принятием закона «О безопасности критической информационной инфраструктуры Российской Федерации». Данный закон также вступил в действие с 01 января 2018 года [26].

В 2022 году Федеральным законом от 14.07.2022 № 260-ФЗ в УК РФ введен новый состав о нарушении правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ) [27].

В литературе до настоящего времени ведется полемика о том, какие действия следует относить к разряду компьютерных преступлений, сложность заключается в широком диапазоне противоправных действий, совершаемых с использованием ЭВМ. Так, например, существует точка зрения, что «компьютерных преступлений как специфических в юридическом смысле преступлений не существует и следует говорить лишь о компьютерных аспектах преступлений» [20, с. 118].

Компьютерные преступления могут наносить ущерб различным субъектам общественных отношений, включая физических лиц, организации и государственные структуры [37, с. 56]. Они могут приводить к нарушению прав на конфиденциальность, целостность и доступность информации, а также к финансовым, экономическим, репутационным и другим видам ущерба.

Общественные отношения в сфере компьютерной информации охраняются законом для обеспечения стабильности, безопасности и правопорядка в цифровом пространстве. Законодательство и правоохранительные органы работают на защиту интересов граждан, организаций и государства, борясь с компьютерными преступлениями и преследуя виновных.

В уголовно-правовой литературе используются различные термины для описания преступлений, связанных с компьютерной информацией. Каждое из этих понятий имеет своё особое содержание и может быть использовано в разных контекстах. Вот некоторые из этих понятий и их общие характеристики. Преступления в сфере компьютерной информации - это общее понятие, которое относится к преступлениям, связанным с использованием компьютеров и цифровых технологий для совершения противоправных действий. Включает в себя различные формы преступлений, такие как несанкционированный доступ к компьютерной информации, киберпреступления, мошенничество, распространение вредоносных программ и т.д.

Компьютерные преступления – данный термин обычно используется для описания преступлений, связанных с использованием компьютеров и информационных систем для совершения противоправных действий [61, с. 72]. Включает в себя различные виды преступлений, такие как хакерство, кража данных, мошенничество в сети, кибершпионаж и т.д.

Киберпреступления могут включать в себя различные формы преступных действий, такие как кибермошенничество, кибернападения, кибершпионаж, распространение вредоносного программного обеспечения и др.

«Преступления в сфере компьютерной информации - это законодательное определение преступлений, предусмотренных главой 28 УК РФ» [38, с. 6].

Таким образом, в доктрине уголовного права компьютерные преступления могут быть представлены:

- как преступления в сфере компьютерной информации;
- информационные компьютерные преступления;
- киберпреступления (интернет-преступления).

К преступлениям в сфере компьютерной информации относятся:

- неправомерный доступ к охраняемой законом компьютерной информации (ст. 272 УК РФ);
- создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ);
- нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ);
- неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ);
- нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования (ст. 274.2 УК РФ).

Таким образом, круг информационных компьютерных преступлений образуют преступления, совершаемые в сфере использования информационно-телекоммуникационных (компьютерных) технологий [59, с. 279]. Это преступления в сфере компьютерной информации, а также иные преступления, которые совершаются в сфере использования информационно-телекоммуникационных (компьютерных) технологий.

Объективная сторона компьютерных преступлений может характеризоваться деянием как в форме действия (например, неправомерный доступ к охраняемой законом информации - ст. 272 УК РФ), так и акта бездействия (например, невыполнение необходимых сервисных процедур,

своевременной антивирусной проверкой - ст. 274 УК РФ).

Материальная сторона преступления относится к внешним проявлениям противоправного деяния, его результатам или последствиям. Она обычно состоит из объективных элементов преступления, таких как действия или бездействие, которые являются запрещенными законом, и их негативные последствия. При преступлениях в сфере компьютерной информации материальная сторона может включать различные виды действий, такие как несанкционированный доступ к компьютерной системе, распространение вредоносных программ, кража данных и т.д. Такие действия могут иметь негативные последствия, такие как утечка конфиденциальной информации, повреждение системы, финансовые потери и т.д.

Причинно-следственная связь между деянием и последствием означает, что последствия являются результатом совершенного преступного деяния. В уголовно-правовом контексте, для признания лица виновным в преступлении, необходимо доказать наличие причинно-следственной связи между его действиями и наступившими последствиями [16, с. 48].

Субъект компьютерных преступлений, предусмотренных в ч. ч. 1 и 2 ст. 272, ч. 1 ст. 273 и ст. 274 УК РФ - общий - физическое вменяемое лицо, достигшее 16 лет. В ч. ч. 3 и 4 ст. 272 и ч. ч. 2 и 3 ст. 273 УК РФ определен специальный субъект как лицо, имеющее в силу своего служебного положения доступ к ЭВМ. В ст. 274.2 УК РФ также специальный субъект – должностное лицо или предприниматель. Субъективная сторона преступлений в сфере компьютерной информации, характеризуется умышленной формой вины.

Таким образом, по результатам главы исследования, предлагаем следующее.

«Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи» [39, с. 24].

Понятие «компьютерная информация» заменить на понятие «электронная информация».

Примечание к ст. 272 УК РФ изложить в следующем виде: «электронная информация» - это любое представление фактов, данных или понятий в форме, подходящей для обработки в устройстве, группе взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных.

Главу 28 УК РФ переименовать в «Преступления в сфере информации, обрабатываемой с использованием электронных устройств».

С развитием информационных технологий и широким использованием компьютеров и сетей в различных сферах, таких как экономика, политика, военное дело и другие, возникают новые возможности для совершения преступлений и нанесения ущерба.

Российское уголовное законодательство в области компьютерных преступлений является отражением текущего состояния правового регулирования в этой сфере. Оно определяет составы преступлений и предусматривает соответствующие санкции. Однако, в силу динамичного развития информационных технологий и появления новых видов преступлений, существующие составы компьютерных преступлений могут оказаться недостаточно эффективными и неспособными полностью удовлетворить требования практики. Дальнейшее совершенствование составов компьютерных преступлений является важной задачей для законодателей и правоохранительных органов. Это может включать расширение понятий, уточнение определений, установление новых видов преступлений и ужесточение санкций для более эффективной борьбы с современными видами компьютерных преступлений.

Однако следует отметить, что развитие законодательства в области компьютерных преступлений должно быть сбалансированным, учитывая, как защиту общества и интересов граждан, так и соблюдение прав и свобод в сфере информационных технологий.

Глава 2 Уголовно-правовая характеристика составов преступлений в сфере компьютерной информации

2.1 Объективные и субъективные признаки основных составов преступлений, предусмотренных ст.ст. 272-274.2 УК РФ

Система признаков состава преступления представлена объективными (объект, объективная сторона) и субъективными (субъект, субъективная сторона) признаками.

Родовым объектом неправомерного доступа к компьютерной информации являются общественные отношения и общественная безопасность. В качестве видового объекта ст. 272 УК РФ можно рассматривать отношения, складывающиеся по поводу правомерного пользования компьютерной информацией.

Объект преступления, предусмотренного ст. 272 УК РФ - общественные отношения, обеспечивающие правомерный доступ, создание, обработку, преобразование и использование охраняемой законом компьютерной информации самим создателем, а также потребление ее иными пользователями. Дополнительным объектом преступления являются личные права и интересы граждан, интересы собственности.

Предметом преступления является компьютерная информация ограниченного доступа. Отметим, что дефиниция компьютерной информации впервые закреплена в федеральном законодательстве. Как объект уголовно-правовой охраны компьютерная информация отвечает трем свойствам: конфиденциальность, целостность и доступность.

Объективная сторона преступления характеризуется неправомерным доступом к охраняемой законом компьютерной информации. Анализ законодательных норм и научных исследований свидетельствует о том, что неправомерный доступ к охраняемой законом компьютерной информации определяется по-разному, ученые предлагают разнообразные определения

данной дефиниции, выдвигая на первый план те или иные аспекты, что не может не вызывать определенных проблем и не свидетельствовать о необходимости выработки единообразного понятия.

В первую очередь, проанализируем законодательные трактовки рассматриваемого понятия, поскольку, как правило, именно наличие легально закрепленных дефиниций позволяет разрешить проблемы и поставить точку в научных диспутах, однако, это возможно лишь в том случае, когда содержащиеся понятия в различных нормативно - правовых документах соответствуют друг другу, не вступая в определенные противоречия, либо в случаях содержания такого определения лишь в одном законодательном акте. К сожалению, в данной сфере такого единообразия не просматривается.

Определение преступлений в сфере компьютерной информации часто включает такие последствия в состав преступления. Законодательство определяет виды преступлений и их элементы, включая как незаконное получение доступа к информации, так и негативные последствия, связанные с этим доступом.

Представляется, что для более правильного понимания термина «неправомерный доступ к компьютерной информации» следует прежде всего рассмотреть вопрос о том, какие действия не следует включать в данное понятие. Так, нельзя рассматривать в качестве неправомерного доступа уничтожение и модификацию компьютерной информации, когда они совершены путем внешнего воздействия на машинные носители, так как, в указанных случаях не будет иметь место какое-либо обращение к компьютерной информации.

«Неправомерным становится доступ, который осуществляется без разрешения ее законного владельца и в нарушение порядка, установленного законодательством» [60, с. 163]. Однако, нами данная позиция разделяется, полагаем, что не имеет значения наличие или отсутствие защиты информации, достаточно того, что она является чужой, то есть, не принадлежащей лицу,

осуществляющему к ней неправомерный доступ, а также то, что она защищается законом.

Не вызывает никаких сомнений тот факт, что существование множества различных определений неправомерного доступа к компьютерной информации, содержащих определенные отличия и разные взгляды на отдельные аспекты, обусловлен недоработкой законодателя, а именно - не закреплением в законе легального определения неправомерного доступа к компьютерной информации.

Поскольку законодатель прямо предусмотрел последствия, которые должны наступить при совершении данного деяния, его состав по своей конструкции является материальным. В то же время нельзя не обратить внимание на тот факт, что законодатель, приведя конкретный перечень общественно опасных последствий, не привел их определений, что не может не вызывать трудностей у правоприменителей. Проанализируем, что же могут представлять собой указанные последствия.

В первую очередь, уделим внимание такому последствию, как уничтожение информации, поскольку оно, с нашей точки зрения, наиболее общественно опасно.

В научной литературе предложено множество толкований данного термина, так, в частности, отмечается, что имеется в виду стирание информации в памяти устройства, физическая ликвидация информации или ликвидация таких ее элементов, которые влияют на изменение существенных идентифицирующих информацию признаков [52, с. 35].

Полагаем, что законодатель подразумевает в данном случае не просто удаление файлов, а необратимую процедуру, не позволяющую в последствии восстановить уничтоженную информацию. В силу этого, целесообразно определять уничтожение информации как ее утрату без возможности восстановления.

Исходя из этого возникает вопрос, на который нет ответа в законодательстве: если информация, после ее уничтожения, через некоторое

время была фрагментарно восстановлена специалистами, то будет ли такое деяние являться уничтожением компьютерной информации.

С.Д. Бражник рассматривает «уничтожение компьютерной информации, при котором не утрачивается возможность ее восстановления, как ее повреждение, и в данном случае состав преступления отсутствует» [15, с. 224].

Ученый считает, что при таких обстоятельствах отсутствует «степень общественной опасности, присущей для преступления» и встает вопрос «о справедливости уголовного наказания за действия, фактически не причинившие существенного вреда владельцу или иному законному пользователю» [53, с. 26].

Блокирование - это также один из признаков объективной стороны такого преступления. При блокировании доступ к компьютерной информации и ее обработка становится невозможной (полностью или частично) для законного пользователя.

Еще одна, достаточно сложная для понимания дефиниция - модификация информации. Данное понятие во многом близко с понятием блокирования, разница заключается лишь в том, что модифицируется управляющая информация, в то время как блокируется - основная. Полагаем, модификация представляет собой внесение любых изменений в информацию, обуславливающих ее отличие от информации владельца. Под модификацией принято понимать такое изменение, усовершенствование, преобразование компьютерной информацией, при которой она получает новые свойства.

На этот счет ученые не всегда дают однозначное толкование этого понятия. Модификацией информации является изменение содержания по сравнению с тем, которое первоначально было в распоряжении законного пользователя или собственника информационного ресурса [55, с. 108]. Важно подчеркнуть, что при квалификации масштабы модификации информации не оказывают никакого влияния, т.к. для привлечения к уголовной ответственности достаточно изменения одного байта информации.

Под копированием информации понимается копирование информации как неправомерное изготовление копий содержания соответствующей информации в любой материальной форме. Полагаем, для целей ст. 272 УК РФ копирование информации следует трактовать как повторение ее в электронном виде помимо или против воли ее законного обладателя.

Состав преступления, предусмотренного ст. 272 УК РФ, являясь материальным, предполагает в обязательном порядке необходимость установления такой связи между действиями - неправомерным доступном к компьютерной информации и последствиями - ее уничтожением, блокированием, модификацией, копированием.

В научной доктрине отмечается, что для того, чтобы была установлена причинная связь, требуется взаимосвязь трех диагностических признаков: в качестве причины может рассматриваться только тот процесс, который имел место до того, как возникло следствие; в качестве причины следует рассматриваться обстоятельство, без которого другое событие не могло бы возникнуть или измениться, причина - всегда необходимое условие следствия; причина и следствие всегда закономерно взаимосвязаны между собой, если имеется причина и условия, которые необходимы для того, чтобы она действовала, ее следствие обязательно наступает [16, с. 48].

В первую очередь, для квалификации содеянного по ст. 272 УК РФ требуется, чтобы неправомерный доступ и наступившие последствия должны обладать между собой закономерной связью, первый должен быть достаточным для наступления вторых и между ними не должно быть третьего звена (к примеру, сбоя в информационной системе).

Например, приговором Кашинского городского суда Тверской области по делу № 1-68/2020 от 21 июля 2020 г., «Журавлев Д.Н. на основании приказа менеджера по поддержке бизнеса Регионального управления Московского региона Публичного акционерного общества «Вымпел-Коммуникации» (далее - ПАО «ВымпелКом») Бабаевой О.Н. от 3 июня 2019 г. №2030-к/мр и трудового договора от 4 июня 2019 г. №7581, заключенного на неопределенный срок между

ПАО «ВымпелКом» - Региональное управление Московского региона в лице генерального директора Лацанича В. и Журавлевым Д.Н., с 4 июня 2019 г. являлся специалистом офиса в офисе обслуживания и продаж в г. Кашин ПАО «ВымпелКом», расположенного по адресу: Тверская область, г. Кашин, ул. Анатолия Луначарского, д. 16/12. При этом, Журавлев Д.Н. прошёл обучение по пользованию компьютерной программой CRM (система регистрации контактов с клиентами), ознакомившись с нормативными документами и требованиями информационной безопасности, получил по итогам обучения индивидуальный и конфиденциальный логин и пароль, необходимые ему для выполнения своих должностных обязанностей. Таким образом, Журавлев Д.Н., имея индивидуальный и конфиденциальный логин и пароль, получил доступ к базе данных, содержащей персональные данные клиентов ПАО «ВымпелКом»» [42].

В один из дней, Журавлев Д.Н. получил от неустановленного лица предложение, согласно которому, за денежное вознаграждение должен был оказать услугу о перевыпуске сим-карты с абонентским номером.

30 августа 2019 г. Журавлев Д.Н. находился на своем рабочем месте в офисе ПАО «ВымпелКом», где у него из корыстной заинтересованности возник прямой преступный умысел, направленный на неправомерный доступ к компьютерной информации, в целях перевыпуска сим-карты с абонентским номером.

При этом, Журавлев Д.Н. осознавал, что перевыпуск сим-карты абонента может быть осуществлен им лишь в офисе обслуживания и продаж в г. Кашин по письменному заявлению абонента.

Реализуя свой преступный умысел, 30 августа 2019 г. Журавлев Д.Н., находясь на своем рабочем месте, используя свою учетную запись, индивидуальный и конфиденциальный логин и пароль на служебном компьютере, предоставленные ему в силу исполнения им должностных обязанностей специалиста офиса обслуживания и продаж в г. Кашин ПАО «ВымпелКом», то есть, используя свое служебное положение, действуя умышлено, незаконно, из корыстных побуждений, не имея законных оснований

на совершение указанных действий, вошёл в программу «1С-Retail», которая используется для внесения изменений в список услуг и проведение абонентских операций с номерами клиентов ПАО «ВымпелКом», тем самым осуществив неправомерный доступ к охраняемой законом информации, где, не имея соответствующего заявления клиента, выбрал абонентский номер, зарегистрированный на М.Е.В., с целью проведения его модификации.

«Продолжая реализацию преступного умысла, 30 августа 2019 г. около 16 часов 30 минут. Журавлев Д.Н., осознавая, что данная информация охраняется Федеральным законом от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и защите информации», осуществил обращение к личной карточке абонента М.Е.В. с номером №, после чего в указанное время, находясь в указанном месте, не имея соответствующего обращения от абонента М.Е.В., произвёл модификацию компьютерной информации лицевой карточки указанного абонента, оформив услугу о получении новой сим-карты, осуществил выдачу сим-карты с указанным абонентским номером, вставил её в свой телефон, активировал, после чего, принял поступившие на указанную сим-карту смс-сообщения и передал их содержание неустановленному в ходе предварительного следствия лицу» [42].

Суд Журавлев Д.Н. признал виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ, и назначил ему наказание в виде ограничения свободы сроком на 1 (один) год 6 (шесть) месяцев.

Объектом создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ) - являются общественные отношения, обеспечивающие безопасность в сфере компьютерной информации. Общественная опасность данного преступления определяется тем, что вредоносные программы способны парализовать работу компьютерной системы, а это может привести к неблагоприятным и даже катастрофическим последствиям.

Основной объект преступлений ст. 273 УК РФ - это общественные отношения, обеспечивающие безопасность в сфере компьютерной информации [49, с. 137].

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

- в создании компьютерных программ либо иной компьютерной информации, заведомо способных приводить к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации;
- использовании компьютерных программ либо иной компьютерной информации;
- их распространении.

«Для признания преступления оконченным не требуется наступления общественно опасных последствий в виде уничтожения, блокирования, модификации или копирования информации» [9, с. 528]. Само получение доступа к информации может быть одним из этапов незаконных действий, но для полного состава преступления необходимы конкретные последствия, связанные с этим доступом. Например, при несанкционированном доступе к компьютерной системе, чтобы считать преступление оконченным, могут потребоваться такие действия, как уничтожение или повреждение данных, блокировка доступа к системе или изменение содержимого информации. Такие последствия могут иметь негативные воздействия на владельца информации или компьютерной системы, вызывая ущерб и нарушение нормального функционирования.

Определение компьютерной программы закреплено в ст. 1261 ГК РФ [13].

Обязательными признаками объективной стороны УК РФ являются два признака, характеризующих способ и средство совершения преступления:

– во-первых, то, что последствия должны быть несанкционированными;
– во-вторых, наличие самой вредоносной программы или иной компьютерной программы.

Компьютерная программа являет собой объективную форму представления совокупности данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств с целью получения определенного результата [4, с. 117].

Под вредоносными программами понимаются специально созданные программы, в том числе модифицированные из невредоносных [21, с. 213].

Преступление, регламентированное ст. 274 УК РФ, с объективной стороны выражается в следующих трех условиях, выполненных одновременно:

– лицо нарушило правила эксплуатации указанного оборудования;
– деяние повлекло уничтожение, блокирование или модификацию компьютерной информации;
– деяние причинило крупный ущерб (свыше 1 млн. руб.).

Объективная сторона преступления, регламентированного ст. 274.1 УК РФ, выражена в создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Понятие критической информационной инфраструктуры Российской Федерации закреплено на уровне федерального законодательства - в вышеназванном ФЗ от 26.07.2017 № 187-ФЗ [24].

Рассматриваемая норма содержит три самостоятельных основных состава преступления. Первый мы уже назвали. Укажем, что в части 2 ст. 274.1

УК РФ предусмотрена ответственность за неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации; в части 3 данной нормы - за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

При этом последствие в виде причинения вреда критической информационной инфраструктуре Российской Федерации - является составообразующим признаком рассматриваемых преступлений [56, с. 103].

Новеллой уголовного законодательстве в сфере противодействия преступлениям в сфере компьютерной информации стала статья 274.2 УК РФ, которая была введена в действие Федеральным законом от 14.07.2022 № 260-ФЗ [27].

На сегодняшний день в России действует почти 4 тысячи операторов связи. Все они, образуя единую сеть, участвуют в обеспечении целостности, и безопасности информационной инфраструктуры страны.

Сейчас каждый оператор связи обязан использовать программно-аппаратный комплекс технических средств противодействия угрозам (далее - ТСПУ) на своих сетях [33]. Это позволяет решать множество задач, в том числе снижать количество информационных угроз путем ограничения доступа к запрещенной на территории РФ информации: экстремистская информация; детская порнография; пропаганда самоубийств; фейковые новости; пронаркотическому контенту.

В случаях отключения ТСПУ или пропуска трафика в обход оборудования, возрастают риски сбоев в работе информационных ресурсов [36].

2022 год показал, что в условиях ведения гибридной войны в отношении России защита информационного пространства страны становится крайне важным. Вот почему необходимо устанавливать новые правила, в которых операторы связи должны пропускать 100% трафика ТСПУ и соблюдать требования по их эксплуатации и модернизации. Все ТСПУ находятся под управлением Центра мониторинга и управления сетью связи общего пользования Роскомнадзора.

Частью 1 статьи 274.2 УК РФ установлена уголовная ответственность за нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенные должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное частью 2 статьи 13.42 Кодекса Российской Федерации об административных правонарушениях (далее – КоАП РФ) [19].

Часть 2 ст. 274.2 вступила в силу с 01.01.2023. Она предусматривает ответственность за нарушение требований к пропуску трафика через ТСПУ, совершенное должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное частью 2 статьи 13.42.1 КоАП РФ.

Непосредственным объектом преступления, предусмотренного частью 1, будет выступать установленный порядок установки, эксплуатации и модернизации в сети связи ТСПУ. В части 2 объектом будет выступать

общественные отношения, обеспечивающие соблюдение требований к пропуску трафика через ТСПУ [36].

Предмет преступления назван в диспозиции - это непосредственно технические средства противодействия угрозам.

«Нормы ст. 274 УК РФ - бланкетные. Поэтому для определения объективной стороны состава преступления необходимо установить, какие именно предписания были нарушены» [2, с. 118].

Для это необходимо обратиться к Правилам установки, эксплуатации и модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, утвержденными постановлением Правительства РФ от 12.02.2020 года № 126 [33], а также требованиям к порядку пропуска трафика в сетях передачи данных утвержденным Приказом Минцифры России от 26.01.2022 № 44 [34].

Установка, эксплуатация и модернизация технических средств противодействия угрозам в сети связи оператора связи осуществляются специально уполномоченной службой по обеспечению регулирования использования радиочастот и радиоэлектронных средств при Роскомнадзоре совместно с уполномоченным представителем оператора связи в соответствии с планом мероприятий. Документом также устанавливаются обязанности операторов связи при эксплуатации ТСПУ.

Таким образом, объективная сторона преступления, предусмотренного частью 1 статьи 274.1 УК РФ, может проявляться:

- в нарушении порядка установки, эксплуатации и модернизации в сети связи ТСПУ;
- несоблюдение технических условий их установки;
- требований к сетям связи при использовании указанных технических средств.

Объективная сторона преступления, предусмотренная частью 2 статьи 274.2 УК РФ, выражается в нарушении требований к пропуску трафика.

Рассмотрим более подробно субъективные признаки данной категории преступлений на примере ст. 272 УК РФ.

Субъект преступления, предусмотренного ч. 1 ст. 272 УК РФ - общий, им признается физическое вменяемое лицо, достигшее 16-ти лет.

При этом, в научной литературе имеется мнение о том, что в данном случае необоснованно расширен круг лиц, которые могут быть привлечены к ответственности по ст. 272 УК РФ.

Так, предлагается ввести дополнительные признаки субъекта указанной нормы, указав, что таковым может являться лицо, не наделенное в силу характера выполняемой им работы полномочиями доступа к компьютерной информации. По мнению исследователей, данная позиция заслуживает внимания, поскольку общественная опасность деяния, совершаемого лицами, не имеющими доступ к компьютерной информации, гораздо выше. Но им предлагается не применять данное правило к субъекту ч. 1 ст. 272 УК РФ, а ввести в данную норму соответствующий признак. В целом, мы разделяем данную позицию, однако, она будет явно противоречить установлению повышенной ответственности за совершение деяния лицом с использованием своего служебного положения.

Также следует отметить имеющееся в научной литературе предложение о снижении возраста уголовной ответственности за рассматриваемое деяние до 14-ти лет. Мы данную позицию полностью разделяем, поскольку нередко подростки в данном возрасте уже вполне профессионально могут обращаться с компьютерной информацией.

Под специальным субъектом преступления понимается лицо, которому присущи как общие признаки субъекта, так и дополнительные, которые рассматриваются в качестве обязательных для конкретного состава преступления [7, с. 102]. Такие признаки прямо называются, либо исходят из толкования нормы. Дополнительные признаки факультативны не для состава

преступления, а для общего понятия субъекта в уголовном праве. Специальный субъект предусмотрен в квалифицированном составе, по ч. 3 ст. 272 УК РФ.

Субъективная сторона отражает психического отношение лица к содеянному. Субъективная сторона данного преступления характеризуется умышленной формой вины по отношению к совершаемым действиям.

Корыстная заинтересованность как обязательный признак субъективной стороны выступает таким при конструкции квалифицированного состава по ч. 2 ст. 272 УК РФ. Приведем пример. Суд с учетом всех материалов дела считает надлежаще установленным наличие указанных в обвинении квалифицирующих признаков - из корыстной заинтересованности, поскольку совершал указанные противоправные действия Данко А.С. для извлечения прибыли, получал денежные средства, что не оспаривается подсудимым и его защитником [45].

В других случаях мотивы и цель преступления могут быть различными, они не выступают конструктивными признаками состава преступление, но могут быть учтены судом при индивидуализации виновному наказания.

Подводя итог, можно отметить следующее. Субъект преступления, предусмотренного ч. 1 ст. 272 УК РФ - общий, им признается физическое вменяемое лицо, достигшее 16-ти лет. При этом, представляется целесообразным снизить данный возраст до 14-ти лет, поскольку нередко подростки в данном возрасте уже вполне профессионально могут обращаться с компьютерной информацией.

С субъективной стороны рассматриваемое преступление характеризуется умышленной формой вины. Вина представляет собой обязательный признак субъективной стороны преступлений, цели и мотивы могут быть разные, как правило, на квалификацию они не оказывают влияния, за исключением корыстной заинтересованности, которая образует квалифицированный состав ст. 272 УК РФ. По отношению к наступлению указанных в законе последствий возможна и неосторожная форма вины.

Содержательное разграничение умышленной и неосторожной форм вины обуславливается различным психическим отношением субъекта деяний к общественной опасности своих действий (бездействия) и наступившим в результате их совершения общественно опасных последствий.

Такое личностное психическое отношение может быть: интеллектуальным; и волевым. Интеллектуальный признак вины представлен: осознанием запрещенности и незаконности своего деяния; а также предвидением общественно опасного результата содеянного.

Субъектом преступлений, предусмотренных ст. 273-274.1 УК РФ, также является вменяемое физическое лицо, достигшее 16-летнего возраста.

Субъект преступления, предусмотренный ст. 274.2 специальный - должностное лицо или индивидуальный предприниматель после его привлечения к административной ответственности по ч. 2 ст. 13.42 КоАП РФ или ч. 2 ст. 13.42.1 КоАП РФ. Аннулирование правовых последствий административного наказания исключает квалификацию деяния по данной статье.

В примечании к статье уточняется, кого следует понимать под должностным лицом - это «лицо, постоянно, временно либо по специальному полномочию выполняющее управленческие, организационно-распорядительные или административно-хозяйственные функции в коммерческой или иной организации» [58].

2.2 Квалифицирующие признаки преступлений в сфере компьютерной информации

В составах преступлений, регламентированных ст.ст. 272-274.1 УК РФ, установлены квалифицирующие и особо квалифицирующие признаки.

Рассмотрим их подробнее.

Ущерб в данных нормах определен как крупный, и применительно к ст. 272 УК РФ превышает 1 млн. рублей.

Квалифицирующим признаком является корыстный мотив. Другие мотивы этого преступления: желание получить какую-нибудь информацию либо желание причинить вред - на квалификацию не влияют.

Согласно приговору Хасавюртовского городского суда Республики Дагестан от 20 июля 2020 г. по делу № 1-261/2020, А. приобрел у неустановленного следствием лица, смарт-карту Триколор ТВ, «предназначенную для подключения через приемник спутникового сигнала к системе спутникового телевидения НАО «Национальная спутниковая компания», на которую из корыстной заинтересованности с целью дальнейшего неправомерного доступа к охраняемой законом компьютерной информации, ее копирования и получения материального вознаграждения, установил вредоносную компьютерную программу на вышеуказанную смарт - карту, предназначенную для несанкционированного доступа к компьютерной информации в виде закодированных ECM-сообщений, оператора спутникового телевидения НАО «Национальная спутниковая компания» [46].

При этом А. было достоверно известно, что при использовании данной вредоносной программы возможен просмотр платных зашифрованных телевизионных спутниковых каналов по технологии, позволяющей осуществлять копирование информации, различных операторов спутникового телевидения, представленной, в том числе, в виде зашифрованных ключевых слов, открывающих доступ к платным зашифрованным спутниковым I телевизионным каналам без оригинальной смарт-карты условного доступа.

В продолжение своего преступного умысла, А. осуществил реализацию указанной выше смарт-карты «Триколор ТВ», установку и настройку через приемник спутникового сигнала к системе спутникового телевидения НАО «Национальная спутниковая компания», за материальное вознаграждение.

В. который выступил в роли условного покупателя, тем самым совершил неправомерный доступ к охраняемой законом компьютерной информации повлекшее ее копирование, причинив тем самым материальный ущерб и вред деловой репутации НАО «Национальная спутниковая компания».

Проверив материалы уголовного дела, суд считает вину подсудимого А. установленной и доказанной полностью, его действия «судом квалифицированы по ч. 2 ст. 273 УК РФ, то есть неправомерный доступ к охраняемой законом компьютерной информации, повлекшее копирование компьютерной информации, совершенное из корыстной заинтересованности, также его действия судом квалифицированы по ч. 2 ст. 272 УК РФ, то есть распространение компьютерной программы, заведомо предназначенной для несанкционированного копирования компьютерной информации совершенное из корыстной заинтересованности.

В следующем примере, согласно данным приговора Далматовского районного суда г. Далматово Курганской области от 20 апреля 2020 года по делу № 1-40/2020., Д., обладая достаточными знаниями в области пользования компьютерной техникой и имея практический опыт работы в сети Интернет, имея преступный умысел на неправомерный доступ к охраняемой законом компьютерной информации, используя свой персональный компьютер с установленной операционной системой, предоставляющей доступ в сеть Интернет, используя известные ему пароль и логин от учетной записи личного кабинета абонента ПАО «Ростелеком» А., осуществил неправомерный доступ к учетной записи личного кабинета А. [40].

При этом Д. изменил пароль для доступа к вышеуказанной учетной записи личного кабинета на подконтрольный ему пароль, с целью ограничения доступа к личному кабинету легального пользователя, и последующего использования его в своих личных корыстных целях.

Затем Д., с целью получения игровой опции игры «World of Tanks» в виде премиум аккаунта и премиум танка, находясь в личном кабинете А. подключил к услуге «Домашний Интернет» свой игровой аккаунт «l_The_HuKoTuH_l» онлайн-игры «World of Tanks» Интернет-ресурса Wargaming.net, введя логин и пароль от своего игрового аккаунта, после чего активировал его.

В результате преступных действий Д. получил на свой игровой аккаунт онлайн-игры «World of Tanks» премиум аккаунт и премиум танк, которые использовал в игре.

Кроме того, в результате неправомерного доступа к компьютерной информации осуществленного Д., в учетной записи личного кабинета абонента ПАО «Ростелеком» А. произошли изменения без ведома и против воли владельца личного кабинета, а именно: изменение пароля для доступа к учетной записи личного кабинета, подключение игровой опции к услуге «Домашний Интернет», которые повлекли модификацию и блокирование для А. охраняемой законом компьютерной информации. Д. неоднократно совершал данные действия.

Д. признан виновным в совершении четырех преступлений, предусмотренных ч. 2 ст. 272 УК РФ.

Особо квалифицирующие признаки, предусмотренные ч. 3 ст. 272 УК РФ, представляют собой совершение данного преступления:

а) группой лиц по предварительному сговору;

б) организованной группой;

в) лицом с использованием своего служебного положения.

Группа лиц по предварительному сговору будет иметь место только в случае, если в преступлении принимали участие два или более лица, которые заранее договорились о совместном совершении преступления. В группу может входить всего один программист-профессионал, а остальные ее члены могут выполнять иные элементы объективной стороны.

Организованная группа, в соответствии с ч. 3 ст. 35 УК РФ характеризуется устойчивостью, более высокой степенью организованности, распределением ролей, наличием организатора и руководителя.

«Под использованием служебного положения понимается осуществление преступных действий лицом, которое в силу занимаемой должности либо выполняемых трудовых обязанностей может использовать ЭВМ, их систему либо сеть. При этом понятие «с использованием служебного положения» шире,

нежели понятие «должностное положение», обусловленное понятием «должностное лицо», определение которого содержится в примечании к ст. 285 УК, так как использование служебного положения включает в себя должностные полномочия, должностной авторитет, иные возможности, предоставленные трудовым договором и административной практикой в той или иной организации» [5, с. 387].

Квалифицирующие признаки могут быть установлены в одном преступлении.

Также приведем пример квалификации по ч. 3 ст. 272 УК РФ. Так, согласно приговору Железнодорожного районного суда, г. Самары от 19 мая 2020 г. по делу № 1-128/2020, М. на основании трудового договора был принят на должность эксперта клиентского сервиса Группы экспертного обслуживания клиентов массового сегмента № Центра клиентского сервиса Филиала публичного акционерного общества «Мобильные ТелеСистемы» [41].

К М. обратилось неустановленное лицо, которое, не ставя последнего в известность о своих истинных намерениях, предложило за денежное вознаграждение предоставлять ему (неустановленному лицу) детализации соединений абонентов ПАО «МТС» посредством их копирования и пересылки на указанную им (неустановленным лицом) электронную почту.

М. принял решение, используя свое служебное положение, при помощи штатного программного обеспечения ПАО «МТС» «Marti», для эксплуатации которого ему были предоставлены персональные логин и пароль, осуществлять неправомерный доступ к охраняемой законом компьютерной информации – персональным данным абонентов ПАО «МТС», а именно сведениям о детализации соединений абонентов, после чего копировать полученную информацию и пересылать посредством использования электронного почтового ящика третьему лицу за денежное вознаграждение, для чего, М., при неустановленных обстоятельствах, получил от неустановленного лица абонентский номер сети ПАО «МТС», что обозначало

необходимость предоставления неустановленному лицу детализации соединений данного абонента за указанный период.

После чего, М., сохранив полученный файл на рабочем столе своего служебного персонального компьютера, затем М., с использованием закрепленной за ним корпоративной электронной почты осуществил отправку незаконно полученной компьютерной информации, скопированной и содержащейся в файле формата «Microsoft Word», на электронную почту неустановленного лица с целью получения денежного вознаграждения. Суд М. признал виновным в совершении преступления, предусмотренного ч. 3 ст. 272 УК РФ.

«Квалифицирующими признаками по ч. 4 ст. 272 УК РФ являются наступление тяжких последствий или опасность их наступления. Это оценочный критерий, хотя, безусловно, к таким последствиям следует относить гибель человека, экологические катастрофы.

К опасности наступления тяжких последствий можно отнести, например, вмешательство в систему управления полетами в аэропорту и нарушение ее работы, не связанное с человеческими жертвами» [1, с. 4].

Применительно к составам преступлений по ст. 273 и 274 УК РФ, квалифицированные (особо квалифицированные) признаки - идентичны.

Приведем пример квалификации по ч. 2 ст. 273 УК РФ из судебной практики. Согласно приговору Хасавюртовского городского суда Республики Дагестан от 18 декабря 2019 г. по делу № 1-386/2019, Г. приобрел у неустановленного лица, смарт-карту «Триколор ТВ, предназначенную для подключения через приемник спутникового канала к системе спутникового телевидения НАО «Национальная спутниковая компания», на которую из корыстной заинтересованности с целью дальнейшего неправомерного доступа к охраняемой законом компьютерной информации, ее копирования и получения материального вознаграждения, установил вредоносную компьютерную программу на вышеуказанную смарт-карту, предназначенную для несанкционированного доступа к компьютерной информации в виде

закодированных ECM-сообщений, оператора спутникового телевидения НАО «Национальная спутниковая компания».

В продолжение своего преступного умысла, из корыстной заинтересованности, Г., в 16 часов 10 минут, в торговом павильоне, расположенном на территории ООО Хасавюртовский универсальный рынок «Дагпотребсоюза», осуществил реализацию указанной выше смарт-карты «Триколор ТВ», установку и настройку через приемник спутникового сигнала к системе спутникового телевидения НАО «Национальная спутниковая компания», за материальное вознаграждение в сумме за 5000 рублей от М.., который выступил в роли условного покупателя, тем самым совершил неправомерный доступ к охраняемой законом компьютерной информации повлекшее ее копирование, причинив тем самым материальный ущерб и вред деловой репутации НАО «Национальная спутниковая компания», после чего сотрудниками отдела «К» БСТМ МВД по РД в ходе проведения оперативно-розыскного мероприятия «проверочная закупка» Г. был задержан [47].

Проверив материалы уголовного дела, суд считает вину подсудимого Г., установленной и доказанной полностью, суд признал Г. виновным в совершении преступлений, предусмотренных ч. 2 ст. 273 УК РФ и ч. 2 ст. 272 УК.

Интересен пример квалификации по совокупности ч. 3 ст. 146 УК РФ и ч. 2 ст. 273 УК РФ. Приведем пример. Так, С., являясь главой компьютерной фирмы, в своем офисе хранил контрафактные экземпляры произведений в целях сбыта в крупном размере [44].

Это были несколько дисков с «ломаными» версиями Autodesk AutoCAD (розничная цена каждой - 70 - 120 тыс. руб.), Microsoft Office (розничная цена - более 20 тыс. руб.). На системном блоке обнаружились программы 1С: Предприятие (12-16 тыс. руб.).

В общей сложности в офисе хранилось контрафакта на общую сумму 515337 руб. Выяснилось это в ходе оперативно-розыскного мероприятия (проверочная закупка), когда предприниматель установил программ на общую

стоимость около 200 тыс. руб., получив взамен денежное вознаграждение в размере 100 руб.

Кроме этого, в офисе были обнаружены скачанные из Интернета вредоносные программы и программы, приводящие к удалению либо замене компьютерной информации и направленные на снятие ограничений использования объектов авторских прав, установленных путем применения программно-технических средств защиты объектов авторского права без разрешения правообладателей.

Более того, он установил эти программы (генераторы ключей, известные многим под именем «keygen») на компьютеры еще одних своих клиентов (которые, видимо, чисто случайно также содействовали проведению проверочной закупки).

В итоге действия предпринимателя были квалифицированы органами предварительного расследования по ч. 3 ст. 146 УК РФ и ч. 2 ст. 273 УК РФ.

От назначения реального наказания в виде лишения свободы С. спасли положительные характеристики, отсутствие судимости, то, что он не состоит на учете у нарколога и психиатра, имеет на иждивении малолетнего ребенка, явился с повинной, признал себя виновным и раскаялся.

Суд назначил наказание в виде лишения свободы, но условно.

Не менее рискуют и «частные» компьютерные мастера, размещающие в Интернете и расклеивающие на столбах объявления о своих услугах. Полицейские периодически практикуют контрольные закупки и с ними: вызывают такого специалиста как бы для оказания услуги - как правило, речь идет о переустановке операционной системы (Windows, от 20 тыс. руб.), причем лучше на нескольких рабочих станциях, лучше от пяти (чтобы на выходе получилось 100 тыс. руб.). И после того, как установка будет закончена и деньги мастером получены, тотчас последует задержание.

Одновременно установить на компьютер и свободно распространяемое ПО (например, пакет Open Office - бесплатный аналог Windows), и контрафакт? Чисто теоретически, если вовремя запустить бесплатную

программу или выключить компьютер, то это затруднит доказывание факта использования «ломаного» ПО. Однако это все равно хранение контрафакта.

Тяжкие последствия - оценочное понятие, наличие их в каждом конкретном случае определяется исходя из особенностей дела. Тяжкие последствия (угроза их наступления) - квалифицирующие признаки также состава преступления, регламентированного ст. 274 УК РФ.

В ст. 274.1 УК РФ законодателем закреплены следующие квалифицирующие признаки: группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, тяжкие последствия.

Их содержание рассмотрены нами выше.

Данные признаки относятся к каждому из самостоятельных деяний, предусмотренных частями 1-3 ст. 274.1 УК РФ.

В диспозиции новой статьи 274.2 УУК РФ квалифицирующие признаки отсутствуют.

Таким образом, значительное число компьютерных преступлений относится к групповым, причем чаще всего речь идет о таких формах группового взаимодействия, как организованная группа или преступное сообщество.

Подводя итоги второй главы можно сделать следующие выводы. Предлагается ввести дополнительные признаки субъекта указанной нормы, указав, что таковым может являться лицо, не наделенное в силу характера выполняемой им работы полномочиями доступа к компьютерной информации.

По мнению исследователей, данная позиция заслуживает внимания, поскольку общественная опасность деяния, совершаемого лицами, не имеющими доступ к компьютерной информации, гораздо выше. Но им предлагается не применять данное правило к субъекту ч. 1 ст. 272 УК РФ, а ввести в данную норму соответствующий признак. В целом, мы разделяем данную позицию, однако, она будет явно противоречить установлению

повышенной ответственности за совершение деяния лицом с использованием своего служебного положения.

Также следует отметить имеющееся в научной литературе предложение о снижении возраста уголовной ответственности за рассматриваемое деяние до 14-ти лет. Мы данную позицию полностью разделяем, поскольку нередко подростки в данном возрасте уже вполне профессионально могут обращаться с компьютерной информацией.

Также можно отметить следующее. Субъект преступления, предусмотренного ч. 1 ст. 272 УК РФ - общий, им признается физическое вменяемое лицо, достигшее 16-ти лет. При этом, представляется целесообразным снизить данный возраст до 14-ти лет, поскольку нередко подростки в данном возрасте уже вполне профессионально могут обращаться с компьютерной информацией.

С субъективной стороны рассматриваемое преступление характеризуется умышленной формой вины. Вина представляет собой обязательный признак субъективной стороны преступлений, цели и мотивы могут быть разные, как правило, на квалификацию они не оказывают влияния, за исключением корыстной заинтересованности, которая образует квалифицированный состав ст. 272 УК РФ. По отношению к наступлению указанных в законе последствий возможна и неосторожная форма вины.

Содержательное разграничение умышленной и неосторожной форм вины обуславливается различным психическим отношением субъекта деяний к общественной опасности своих действий (бездействия) и наступившим в результате их совершения общественно опасных последствий.

Также рассмотрев судебную практику, можно сделать вывод, что значительное число компьютерных преступлений относится к групповым, причем чаще всего речь идет о таких формах группового взаимодействия, как организованная группа или преступное сообщество.

Глава 3 Практика квалификации и совершенствование ответственности за преступления в сфере компьютерной информации

3.1 Особенности квалификации преступлений в сфере компьютерной информации (на основе анализа материалов судебной практики)

Увеличение числа пользователей («виртуализация» жизнедеятельности) открыло новые возможности и для преступной деятельности.

Для борьбы с киберпреступностью важно принимать меры как на государственном уровне, так и на уровне отдельных организаций и отдельных лиц. Государства должны разрабатывать и усовершенствовать законы, регулирующие киберпреступность, и создавать специализированные органы для расследования и пресечения таких преступлений.

С развитием мобильных устройств и приложений, появляются новые виды киберпреступлений, связанных с мобильной сферой. Например, вредоносные программы, разработанные специально для атак на мобильные устройства, мошенничество с использованием мобильных платежных систем и фишинг через мобильные приложения. Преступники также могут использовать мобильные устройства для хранения и распространения незаконного контента, такого как детская порнография или наркотики.

Построение информационно-коммуникационной инфраструктуры закономерно вызвало появление новых форм общественно опасного поведения личности - компьютерной преступности (computer crime) [50, с. 73]. Необходима серьезная системная работа.

Так, ряд исследователей скептически отнеслись к криминализации мошенничества в сфере компьютерной информации (ст. 159.6 УК РФ) [54, с. 273].

Пленум высшей судебной инстанции отметил, что 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 [30].

Научному сообществу и законодателю еще потребуется оценить необходимость криминализации DDoS-атаки [10, с. 164], спаминга, фишинга и др.

Обязательно нужно осуществлять фиксацию IP-адресов (своими силами, силами сторонних организаций, осуществляющих защиту от атак, или силами провайдера), участвовавших в компьютерной атаке на информационный ресурс или на сервер [14, с. 36].

Данные действия существенно повысят вероятность установления организатора атаки и механизма ее организации (как следует из постановления суда от 25.11.2013 по делу № 10-11502/2013 по ч. 2 ст. 272 УК РФ) [3].

При появлении подозрений о совершении атаки надлежит осуществить блокирование счетов, доступ к которым возможен посредством сети Интернет, поскольку злоумышленник, имеющий целью хищение денежных средств с помощью полученной информации, постарается совершить его незамедлительно (определение суда от 24.04.2013 по делу № 22-2480 по ст. 273 УК) [18].

Анализ практики показывает, что нередко компьютерные преступления совершаются и позже квалифицируются в совокупности.

Приведем пример [43]. Б.С. Арсланбекову было достоверно известно, что после использования данной вредоносной программы возможен просмотр платных закодированных телевизионных цифровых спутниковых каналов по технологии, позволяющей осуществлять копирование информации, охраняемой Федеральным законом № 149-ФЗ от 27 июля 2006 года «Об информации, информационных технологиях и защите информации», различных операторов спутникового телевидения, представленной, в том

числе, в виде зашифрованных ключевых слов, открывающих доступ к платным закодированным телевизионным цифровым спутниковым каналам без оригинальной смарт-карты условного доступа.

Программное обеспечение, предназначенное для копирования компьютерной информации операторов спутникового телевидения, используется по следующей схеме: компьютерная информация, содержащая, в том числе, зашифрованные ключевые слова, поступает на ресивер, который передает ее через ГИС Интернет к специализированному серверу, где в режиме реального времени без ведома оператора спутникового телевидения происходит расшифровка ключевых слов, необходимых для просмотра платных зашифрованных спутниковых телеканалов.

Расшифрованные ключевые слова, поступившие обратно на ресивер, дают возможность пользователю незаконно просматривать закрытые каналы, при этом пользователь вносит соответствующую абонентскую плату не определенному оператору спутникового телевидения, а владельцу специализированного сервера, которая существенно ниже, чем стоимость услуг оператора спутникового телевидения.

В последующем, Б.С. Арсланбеков, доводя задуманное до логического конца, путем подключения вышеуказанного ресивера к телевизору, установленному у себя дома, не позднее января 2017 года, удостоверился о неправомерном переносе компьютерной информации путем копирования, тем самым получил незаконный доступ к просмотру платных каналов спутникового телевидения ООО «НТВ-ПЛЮС», причинив вред их деловой репутации. Своими действиями Б.С. Арсланбеков осуществил неправомерный доступ к охраняемой законом компьютерной информации, повлекший копирование компьютерной информации, из корыстной заинтересованности.

Он же, Б.С. Арсланбеков, реализуя свой преступный умысел, не позднее конца января 2017 года, при неустановленных обстоятельствах, умышленно, из корыстной заинтересованности, с помощью своего персонального компьютера разместил на сайте «Авито» информацию о предоставляемых им

платных услугах по изменению программного обеспечения спутниковых ресиверов для просмотра платных зашифрованных телевизионных спутниковых каналов. Получив информацию об этом, в целях пресечения указанной преступной деятельности Б.С. Арсланбекова, сотрудники отдела «К» МВД приступили к проведению оперативного мероприятия «Проверочная закупка», к которой был привлечен оперативный сотрудник Д.М. Абачараев, выступавший в роли условного покупателя.

В ходе проведения данного оперативно-розыскного мероприятия между Д.М. Абачараевым и Б.С. Арсланбековым по телефону была достигнута договоренность о том, что последний за денежное вознаграждение в сумме 4 000 рублей окажет услугу по изменению программного обеспечения и настройке ресивера фирмы «GI HD», после которой он будет способен осуществлять прием платных зашифрованных телевизионных спутниковых каналов ООО «НТВ-ПЛЮС».

Таким образом, своими действиями Б.С. Арсланбеков распространил и использовал компьютерную программу, заведомо предназначенную для несанкционированного копирования компьютерной информации, из корыстной заинтересованности.

В суде подсудимый полностью признал себя виновным. Судом его действия квалифицированы по ч. 2 ст. 272 и ч. 2 ст. 273 УК РФ.

Практика привлечения к ответственности по ст. 274.1 УК РФ - находится в стадии своего становления.

На сегодняшний день ни одного преступления по статье 274.2 не зарегистрировано, поэтому говорить об эффективности новеллы пока рано.

3.2 Направления совершенствования уголовной ответственности за преступления в сфере компьютерной информации

С увеличением использования компьютерных технологий и интернета во всех сферах жизнедеятельности, преступления, связанные с неправомерным оборотом компьютерной информации, становятся все более распространенными во всем мире.

Это может включать в себя различные виды киберпреступлений, такие как хакерство, фишинг, мошенничество с использованием платежных систем и другие формы компьютерной преступности [63, с. 187].

В действующем уголовном законе непосредственно таким деяниям посвящена гл. 28 УК РФ, которая включает пять статьей.

Согласно статистическим сведениям ФКУ «ГИАЦ МВД России», число зарегистрированных преступлений, предусмотренных ст. 272 УК РФ, в 2019 г. составило 1761, в 2020 г. - 2420, а в 2022 г. – 4105 [35]. Как видно из показателей, пандемия COVID-19 и связанные с ней ограничительные мероприятия существенным образом повлияли на компьютерную преступность.

Количество зарегистрированных случаев создания, использования и распространения вредоносных компьютерных программ (ст. 273 УК РФ) в 2020 г. составило 733, в 2021 г. - 455, в 2022 г. - 371 [35]. В значительно меньшем объеме фиксируется число преступлений, предусмотренных ст. 274 УК РФ [35].

Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК РФ) была установлена лишь в середине 2017 г. Но с этого момента норма уже нашла отражение в практической деятельности. В 2018 г. было зарегистрировано одно преступление, в дальнейшем сформировалась тенденция к росту числа таких деяний.

Причины роста таких преступлений могут быть связаны с развитием научно-технического прогресса, который создает новые возможности и инструменты для киберпреступников. Быстрый рост числа людей, использующих электронные средства платежа и приложения, работающие через интернет, также создает больше возможностей для совершения преступлений в сети.

В настоящее время составы преступления, предусмотренные ст.ст. 272-274.2 УК РФ, не включают в качестве конструктивного или квалифицирующего признака цель скрыть другое преступление или облегчить его совершение.

Полагаем возможным согласиться с мнением о том, что «отсутствие в уголовном законе прямого указания на обязательность анализа мотивов и целей совершения компьютерных преступлений является пробелом в законодательстве» [8, с. 232]. «Если первые случаи неправомерного доступа к компьютерной информации и создания вредоносных программ осуществлялись из хулиганских побуждений, то в настоящее время они направлены на достижение конкретных целей, и это необходимо учитывать при дифференциации уголовной ответственности. Достаточно обратить внимание на сферу электронной коммерции, с развитием которой неизбежно возрастают риски компьютерных атак, направленных на клиентов» [8, с. 232-233].

Цель скрыть другое преступление или облегчить его совершение давно известна уголовному праву. Это явление выступает в качестве обстоятельства, отягчающего наказание (п. «е.1» ч. 1 ст. 63 УК РФ). Но в ряде случаев законодатель обоснованно посчитал необходимым закрепить такой признак в качестве квалифицирующего, например, при совершении убийства (п. «к» ч. 2 ст. 105 УК РФ) или подделки документов, государственных наград, штампов, печатей или бланков (ч. 4 ст. 327 УК РФ). Закрепление указанной цели в киберпреступлениях также представляется оправданным.

Также можно выявить еще одну проблему уголовно-правового регулирования противодействия компьютерным преступлениям. В настоящее время диспозиция ст. 273 УК РФ предусматривает такие виды деяний, как создание, распространение или использование вредоносных программ. Поскольку основной состав данного преступления по конструкции объективной стороны является формальным, момент его окончания связывается с совершением вышеуказанных действий.

«Существует множество авторских определений создания вредоносной программы. Например, под данным действием понимается комплекс операций, состоящий из подготовки исходных данных, предназначенных для управления конкретными компонентами системы обработки данных в целях уничтожения, блокирования, модификации или копирования информации» [8, с. 234]. Встречаются иные определения, в том числе довольно дискуссионного характера. Однако все формулировки сводятся к тому, что описываются деяния, направленные на возникновение вредоносной программы, которая ранее не существовала или не обладала вредоносными функциями. По мнению законодателя, сам факт создания программы уже является общественно опасным поведением, хотя ее использование или распространение могло не осуществляться. В то же время «владение лицом вредоносным программным обеспечением может быть осуществлено не только посредством его создания, но и с использованием других способов, не отраженных в уголовном законодательстве. Так, в частности, возможны покупка, обмен, получение в дар, скачивание и другие варианты» [8, с. 234].

Вместе с тем как создание, так и приобретение вирусов может осуществляться в научных, учебных, экспертных и иных некриминальных целях. Буквальное толкование ст. 273 УК РФ (а тем более с учетом возможной криминализации приобретения) не исключает уголовной ответственности в таких случаях, хотя общественная опасность отсутствует. То есть запрещено любое умышленное создание, использование и распространение вредоносных программ. Положения о малозначительности деяния (ч. 2 ст. 14 УК РФ) также

не всегда применимы, поскольку не имеют четко выраженных критериев и используются на практике чрезвычайно редко. В европейском законодательстве, к слову, такая проблема тоже имеет место. Исследователи отмечают необходимость какой-либо правовой защиты в случае хакерства в общественно полезных целях [62].

Возвращаясь к вопросу совершенствования уголовно-правового регулирования преступлений в сфере компьютерной информации, считаем целесообразным включить в диспозицию ст. 273 УК РФ указание на противоправность действий с помощью прилагательного «незаконные».

Не возникает сомнений, что цель скрыть другое преступление или облегчить его совершение повышает общественную опасность преступлений в сфере компьютерной информации, как и лиц, их совершающих. Изучение актуальной судебной практики показало, что такая цель имеет место достаточно часто.

В науке уголовного права уже предлагались рекомендации по совершенствованию ст. 272 УК РФ с дополнением ее признаком, учитывающим цель скрыть другое преступление или облегчить его совершение. Для обеспечения системности совершенствования уголовного закона изменениям должна подвергнуться ст. 273 УК РФ.

Приобретение вредоносных программ не менее общественно опасное деяние, чем их создание. Таким образом, действующие положения уголовного закона о преступлениях в сфере компьютерной информации нуждаются в изменениях. Недостатком действующего законодательства видится отсутствие законодательного определения тех терминов, которые перечислены в ч. 1 ст. 272 УК РФ в качестве преступных последствий.

Представляется целесообразным закрепить понятия уничтожение, блокирование, модификация и копирование информации, в примечании к ст. 272 УК РФ, что позволит исключить трудности в понимании и толковании данных терминов и будет способствовать единообразию судебной практики.

Также необходимо отметить отсутствие легально закрепленного определения неправомерного доступа к компьютерной информации, что порождает множество разнообразных взглядов на рассматриваемую проблему.

Несмотря на то, что наиболее активно данные вопросы рассматривались достаточно давно, когда начала действовать рассматриваемая норма и появились проблемы при ее применении, они не утратили своей актуальности до настоящего времени. Очевидно, что все эти проблемы необходимо решать в кратчайшие сроки в силу того, что отсутствие законодательно закрепленной дефиниции всегда влечет за собой множество проблем и дискуссий.

Подводя итоги по третьей главе исследования, на основе анализа различных точек зрения, высказанных в научной литературе, а также в нормативно-правовых актах, представляется возможным определить неправомерный доступ к компьютерной информации как несанкционированное обращение к ней, дающее возможность получить данную информацию (ознакомиться с ней) и (или) использовать ее. При этом, для того чтобы данное определение было возможно унифицировано использовать, видится необходимым внести изменения в ч. 1 ст. 272 УК РФ, дополнив ее термином «ознакомление», как одним из видов последствий, который может наступить в результате неправомерных действий лица.

Считаем возможным предложить вариант ч. 1 и ч. 2 ст. 273 УК РФ с учетом разработанных нами изменений:

«1. Незаконные приобретение, 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, - …»

В свою очередь, квалифицированный состав, предусмотренный ч. 2 ст. 273 УК РФ, примет следующий вид:

«2. Деяния, предусмотренные частью первой настоящей статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности либо совершенные с целью скрыть другое преступление или облегчить его совершение, - …»

На сегодняшний день ни одного преступления по статье 274.2 УК РФ не зарегистрировано, поэтому говорить об эффективности новеллы пока рано. Тем не менее, сам факт внесения этих изменений в административное и уголовное законодательство демонстрирует готовность законодателя к дальнейшему реформированию главы 28 УК РФ с целью обеспечить информационную безопасность государства. И все же, установление уголовной ответственности за административную преюдицию видится не совсем правильным. Такая формулировка диспозиций встретила справедливую критику еще на этапе обсуждения законопроекта в Государственной Думе. Большинство ученых-правоведов негативно относятся к ее применению в качестве криминообразующего признака в уголовном законе [23, с. 101].

Использование административной преюдиции для криминализации деяний приводит к тому, что в качестве единичного преступления объявляются несколько административных правонарушений, даже не имеющих между собой внутренней связи. Таким образом, считает правильным исключить из текста статьи 274.2 УК РФ требование о первичном привлечении лица к административной ответственности. Статистические данные указывают на актуальность и востребованность норм, предусмотренных главой 28 Уголовного кодекса Российской Федерации, которая регулирует компьютерные преступления. Однако, также отмечается наличие некоторых недостатков в уголовно-правовом регулировании и необходимость их устранения для повышения эффективности привлечения к ответственности и более широкого охвата общественно опасных действий.

Заключение

Развитие компьютерных технологий и распространение их использования на планшетах, смартфонах и других устройствах приводит к тому, что преступники находят новые способы использования этих технологий в своих криминальных действиях. Это создает новые вызовы для правоохранительных органов и общества в целом, и связано с необходимостью адаптации законодательства к новым вызовам и угрозам, связанным с компьютерной информацией и информационными технологиями.

По проведенному исследованию можно сформулировать следующие выводы.

Понятие «компьютерная информация» заменить на понятие «электронная информация».

Примечание к ст. 272 УК РФ изложить в следующем виде: «электронная информация» - это любое представление фактов, данных или понятий в форме, подходящей для обработки в устройстве, группе взаимосвязанных или смежных устройств, одно или более из которых, действуя в соответствии с программой, осуществляет автоматизированную обработку данных, включая программы, способные обязать такие устройства выполнять ту или иную функцию.

Главу 28 УК РФ переименовать в «Преступления в сфере информации, обрабатываемой с использованием электронных устройств».

Нельзя не обратить внимания на то, что устойчивая тенденция возрастания общественной опасности компьютерных преступлений обусловлена стремительным расширением сфер использования информационных технологий и, в частности компьютерной техники экономической, политической, военной областях и др. Соответственно, российской уголовное законодательство в данной сфере не в полной мере отвечает потребностям практики и требует дальнейшего совершенствования составов компьютерных преступлений.

Представляется, что для более правильного понимания термина «неправомерный доступ к компьютерной информации» следует прежде всего рассмотреть вопрос о том, какие действия не следует включать в данное понятие. Так, нельзя рассматривать в качестве неправомерного доступа уничтожение и модификацию компьютерной информации, когда они совершены путем внешнего воздействия на машинные носители, так как, в указанных случаях не будет иметь место какое-либо обращение к компьютерной информации.

Представляется целесообразным закрепить понятия уничтожение, блокирование, модификация и копирование информации, в примечании к ст. 272 УК РФ, что позволит исключить трудности в понимании и толковании данных терминов и будет способствовать единообразию судебной практики.

Также необходимо отметить отсутствие легально закрепленного определения неправомерного доступа к компьютерной информации, что порождает множество разнообразных взглядов на рассматриваемую проблему.

Предлагаем определить неправомерный доступ к компьютерной информации как несанкционированное обращение к ней, дающее возможность получить данную информацию (ознакомиться с ней) и (или) использовать ее.

При этом, для того чтобы данное определение было возможно унифицировано использовать, видится необходимым внести изменения в ч. 1 ст. 272 УК РФ, дополнив ее термином «ознакомление», как одним из видов последствий, который может наступить в результате неправомерных действий лица.

Считаем правильным исключить из текста статьи 274.2 УК РФ требование о первичном привлечении лица к административной ответственности.

Список используемой литературы и используемых источников

1. Аветисян С.С. Уголовно-правовая характеристика ст. 272 УК РФ // Синтез науки и общества в решении глобальных проблем современности. Уфа:МЦИИ. 2016. С. 3-4.

2. Алякин С.С., Дубин А.С., Прокофьева А.В. Уголовно-правовой анализ статьи 274.2 УК РФ и перспективы ее применения в контексте информационных угроз // Научное сообщество студентов. Междисциплинарные исследования. Новосибирск : Общество с ограниченной ответственностью «Сибирская академическая книга», 2023. С. 115-120.

3. Апелляционное постановление Московского городского суда по делу № 10-11502/2013 от 25.11.2013 года // [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

4. Болтуева М.Я. К вопросу о правовой природе категории «компьютерная программа» // Вестник Таджикского государственного университета права, бизнеса и политики. Серия общественных наук. 2018. № 2. С. 113-120.

5. Борзенков Г.Н., Комисаров В.С. Курс уголовного права в пяти томах. Том 4. Особенная часть М. : Зерцало. 2002. 437 с.

6. Бундин М.В. Система информации ограниченного доступа и конфиденциальность // Вестник Нижегородского университета им. Н.И. Лобачевского. 2015. № 1. С. 120-130.

7. Воловик Ю. В. Признаки субъекта преступления // Молодой ученый. 2019. № 52 (290). С. 100-102.

8. Гладких В.И., Мосечкин И.Н. Проблемы совершенствования уголовно-правовых мер противодействия преступлениям в сфере компьютерной информации // Всероссийский криминологический журнал. 2021. № 2. С. 229-237.

9. Гобозов А.З. Проблема разграничения неправомерного доступа к охраняемой законом компьютерной информации от смежных составов преступления // StudNet. 2020. № 9. С. 526-532.

10. Голубев М.Д. К вопросу о необходимости криминализации деяний в форме целевых хакерских атак // Молодой ученый. 2018. № 13 (199). С. 164-165.

11. ГОСТ 15971-90 «Системы обработки информации. Термины и определения» от 26 октября 1990 г. № 2698 [Электронный ресурс]. URL.: https://docs.cntd.ru/ (дата обращения 25.01.2023).

12. Гражданский кодекс Российской Федерации (часть первая) от 30.11.1994 № 51-ФЗ (ред. от 16.04.2022) [Электронный ресурс] URL: http://www.consultant.ru (дата обращения: 25.01.2023).

13. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 № 230-ФЗ (ред. от 05.12.2022) [Электронный ресурс] URL: http://www.consultant.ru (дата обращения: 25.01.2023).

14. Дьяченко Н.С., Беккалиева Н.К. Проблемы оценки экономического ущерба кибератак // Современное состояние и перспективы развития науки и образования. Анапа : Изд-во «НИЦ ЭСП» в ЮФО, 2019. С. 29-37.

15. Зубова М. А. Неправомерный доступ к компьютерной информации и его последствия // Проблемы экономики и юридической практики. 2007. № 3. С. 223-225.

16. Игнатьев М. Е. Криминалистическое значение уголовно-правовой причинной связи // Проблемы правоохранительной деятельности. 2017. № 1. С. 48-53.

17. Какорин И. А. Основные принципы информационной безопасности // Международный журнал гуманитарных и естественных наук. 2023. № 2-2 (77). С. 25-27.

18. Калюжная А. Н., Шарыпова Т. Н. Проблема определения ущерба в результате кибератаки // Аллея науки. 2019. Т. 4, № 1(28). С. 900-903.

19. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 № 195-ФЗ (ред. от 28.02.2023) [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 25.01.2023).

20. Ловцов Д.А. Системология правового регулирования информационных отношений в инфосфере: Монография. М. : РГУП, 2016. 316 с.

21. Логвинова И.А., Сафонова К.Р., Сапрыкина А.Ю. Актуальные вопросы, связанные с созданием, использованием и распространением вредоносных компьютерных программ // Право, как искусство добра и справедливости. Курск : Юго-Западный государственный университет, 2022. С. 211-215.

22. Лысов А.А., Яковлев А.В., Клочкова А.Л. Гистерезис понятия «компьютерная информация» в уголовном законодательстве Российской Федерации // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. 2022. № 1(140). С. 132-135.

23. Мамхягов З.З Об административной преюдиции в уголовном законодательстве // Общество и право. 2016. № 1 (55). С. 100-102.

24. О безопасности критической информационной инфраструктуры Российской Федерации [Электронный ресурс] : Федеральный закон от 26.07.2017 № 187-ФЗ (последняя редакция). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

25. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации [Электронный ресурс]: Федеральный закон от 07.12.2011 № 420-ФЗ (последняя редакция). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

26. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный

ресурс] : Федеральный закон от 26.07.2017 № 194-ФЗ (последняя редакция). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

27. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации [Электронный ресурс] : Федеральный закон от 14.07.2022 № 260-ФЗ (последняя редакция). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

28. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть «Интернет»: Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 // Бюллетень Верховного Суда РФ. 2023. № 3.

29. О ратификации Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации [Электронный ресурс] : Федеральный закон от 01.10.2008 № 164-ФЗ (последняя редакция). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

30. О судебной практике по делам о мошенничестве, присвоении и растрате: Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 (ред. от 15.12.2022) // Российская газета. 2017. № 280.

31. Об информации, информатизации и защите информации [Электронный ресурс] : Федеральный закон от 20.02.1995 № 24-ФЗ (утратил силу). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

32. Об информации, информационных технологиях и о защите информации [Электронный ресурс] : Федеральный закон от 27.07.2006 № 149-ФЗ (ред. от 29.12.2022). URL.: http://www.pravo.gov.ru (дата обращения: 10.03.2023).

33. Об установке, эксплуатации и о модернизации в сети связи оператора связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской

Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования [Электронный ресурс] : Постановление Правительства РФ от 12.02.2020 № 126 (ред. от 28.05.2022). URL.: https://www.consultant.ru/ (дата обращения: 10.03.2023).

34. Об утверждении Требований к порядку пропуска трафика в сетях передачи данных: приказ Минцифры России от 26.01.2022 № 44 // Официальный интернет-портал правовой информации [Электронный ресурс]. URL.: http://pravo.gov.ru (дата обращения 25.01.2023).

35. Официальный сайт Министерства внутренних дел РФ [Электронный ресурс]. URL.: https://мвд.рф/ (дата обращения 25.01.2023).

36. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций [Электронный ресурс]. URL.: https://41.rkn.gov.ru/ (дата обращения 25.04.2023).

37. Петрова И.А., Лобачев И.А. Преступления в сфере компьютерной (цифровой) информации: дискуссионные вопросы определения понятия, объекта уголовно-правовой охраны и предмета посягательств // Журнал прикладных исследований. 2020. № 1. С. 52-62.

38. Попов А.Н. Преступления в сфере компьютерной информации: учебное пособие. Санкт-Петербург : Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.

39. Поспех Р.О. Компьютерная информация как объект преступления // Новый юридический вестник. 2021. № 2 (26). С. 24-27.

40. Приговор Далматовского районного суда г. Далматово от 20 апреля 2020 г. по делу № 1-40/2020 [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

41. Приговор Железнодорожного районного суда г. Самары от 19 мая 2020 г. по делу № 1-128/2020 [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

42. Приговор Кашинского межрайонного суда Тверской области от 21 июля 2020 г. по делу № 1-68/2020 [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

43. Приговор Ленинского районного суда г. Махачкалы от 4 июля 2017 года по делу № 1-316/2017 [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

44. Приговор Ленинского районного суда г. Оренбурга по делу № 1-538/2020 от 23 июля 2020 года [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

45. Приговор Петушинского районного суда Владимирской области по делу № 1-85/2020 от 2 июля 2020 года [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

46. Приговор Хасавюртовского городского суда Республики Дагестан г. Хасавюрт по делу № 1-261/2020 от 20 июля 2020г. [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

47. Приговор Хасавюртовского городского суда Республики Дагестан от 18 декабря 2019 г. по делу № 1-386/2019 [Электронный ресурс]. URL.: https://sudact.ru/ (дата обращения 25.01.2023).

48. Рамлова С.С. Современные внешние устройства хранения информации и методы их исследования в компьютерно-технической экспертизе (КТЭ) // Криминологический журнал. 2021. №4. С. 89-93.

49. Репьева Е.О. О некоторых проблемах определения непосредственного объекта ст. 273 УК РФ // Вестник науки. 2019. Т. 3, № 11(20). С. 136-138.

50. Русскевич Е.А. Уголовное право и информатизация // Журнал российского права. 2017. № 8. С. 73-80.

51. Солнцев М.Н. Криминологическая характеристика преступлений в сфере компьютерной информации" // Вестник государственного и муниципального управления. 2012. № 1. С.99-102.

52. Сотов А.И. Компьютерная информация под защитой. Правовое и криминалистическое обеспечение безопасности компьютерной информации: монография. Москва : Ru-science.com, 2017. 127 с.

53. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: Монография. М. : Статут, 2016. 190 с.

54. Стилиди Д.П. Мошенничество в сфере компьютерной информации как состав преступления: проблемы квалификации и правоприменения // Молодой ученый. 2021. № 49 (391). С. 272-274.

55. Суханова И. Ю. Проблемы квалификации неправомерного доступа к компьютерной информации // Распространение недостоверной информации как угроза безопасности граждан, общества и государства. Воронеж: Автономная некоммерческая организация по оказанию издательских и полиграфических услуг «Наука-Юнипресс», 2023. С. 106-109.

56. Трунцевский Ю.В. Неправомерное воздействие на критическую информационную инфраструктуру: уголовная ответственность ее владельцев и эксплуатантов // Журнал российского права. 2019. № 5. С. 99-106.

57. Уголовное право. Особенная часть: учебник для вузов/ под общ. ред. Л.М. Прозументова. - Томск : Издательский Дом Томского государственного университета, 2019. 844 с.

58. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 29.12.2022). [Электронный ресурс]. URL: http://www.consultant.ru (дата обращения: 25.01.2023).

59. Унукович А.С. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Государственная служба и кадры. 2021. № 4. С. 278-280.

60. Харламова А.А. Неправомерный доступ к компьютерной информации: толкование признаков и некоторые проблемы квалификации // Вестник Уральского юридического института МВД России. 2020. № 2. С. 162-167.

61. Чакрян В.Р., Кешишян В. В. Понятие компьютерных преступлений и их классификация // Символ науки, 2020. № 12-2. С. 71-75.

62. Guinchard A. The Computer Misuse Act 1990 to Support Vulnerability Research Proposal for a Defence for Hacking as a Strategy in the Fight against Cybercrime // Journal of Information Rights, Policy and Practice. 2017. Vol. 2, iss. 1.

63. Li X. Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime // International Journal of Cyber Criminology. 2020. Vol. 9, iss. 2. P. 185-204.