МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
«ТЮМЕНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ГОСУДАРСТВА И ПРАВА
Кафедра уголовного права и процесса

РЕКОМЕНДОВАНО К ЗАЩИТЕ
В ГЭК
И.о. заведующего кафедрой
канд. юрид. наук, доцент
В.И. Морозов
02.12. 2019 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**
магистра

# ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ЗАКОН, ТЕОРИЯ, ПРАКТИКА

40.04.01 направление подготовки Юриспруденция
Магистерская программа «Уголовное право, уголовный процесс»


Выполнил работу
студент 3 курса
заочной формы
обучения
Косогоров
Егор
Михайлович

Научный руководитель
д-р юрид. наук, профессор
Сумачев
Алексей
Витальевич

Рецензент
профессор кафедры
информационно-аналитического
и документационного
обеспечения деятельности
органов внутренних дел ТИПК
МВД, д-р юрид. наук, профессор
Юзиханова
Эльвира
Гумеровна


Тюмень
2019

# ВВЕДЕНИЕ

**Актуальность темы исследования.** В связи с активизацией развития информационных технологий, интенсивно внедряющихся в общество, одной из самых актуальных задач правовой доктрины и судебно-следственной практики становится совершенствование правовой регламентации общественных отношений, складывающихся в области создания и обеспечения информационной безопасности. Подавляющее большинство направлений современной человеческой деятельности в той или иной степени связана с компьютерами. Информационные технологии вошли в различные сферы жизни (в оборону, экономику, промышленность, транспорт, образование, культуру, медицину и пр.). Развитая информационная инфраструктура способствует социально-экономическому прогрессу, созданию и распространению научно-технической информации. Объединение компьютеров в сети дает возможность быстрого обмена информацией между пользователями в любом месте земного шара.

В настоящее время в мире насчитывается 3,2 млрд. пользователей Интернета (все население планеты Земля насчитывает около 7,2 миллиардов человек), из них 2 млрд. проживают в развивающихся странах. В период с 2010 по 2019 г. удельный вес пользователей сети Интернет увеличился почти в семь раз - с 6,5 до 43% мирового населения [111]. За последние годы Интернет прочно вошел в повседневную и деловую жизнь страны. Россия не отстает и не остается в стороне от глобальных трендов. Российская аудитория Интернета крупнейшая в Европе, она превышает 80 млн. пользователей, из них 62 млн. человек выходят в сеть ежедневно [111].

Однако компьютеризация общества влечет не только положительные, но и отрицательные стороны. Отмечается, что современные информационно-коммуникационные технологии стали все чаще использоваться для военно-политического противоборства. Кроме того, интернет-технологии взяли на

вооружение террористы и преступники. Со всеми этими проблемами многие страны сталкиваются уже постоянно. Эти угрозы нельзя игнорировать.

По данным Министерства внутренних дел РФ, в 2006 г. было зарегистрировано 8889 преступлений в сфере компьютерной информации (7337 - ст. 272 Уголовного кодекса Российской Федерации (далее - УК РФ), 1549 - ст. 273 УК РФ и 3 - ст. 274 УК РФ); в 2010 г. - 7236; в 2011 г. - 9010; в 2012 г. - 11 636; в 2013 г. - 7398; в 2014 г. - 2698; в 2015 г. - 2820; в 2016 г. - 2563; в 2017 г. – 1739; в 2018 г. – 2142 [111].

Для выработки эффективных мер борьбы с данным видом преступлений необходимо продолжать исследовать теорию и практику применения законодательства о компьютерных преступлениях. Настоящая работа посвящена анализу общественных отношений, определяющих комплекс теоретических проблем уголовного права, а также обобщению практики применения норм уголовного законодательства, устанавливающего ответственность за преступные посягательства в сфере компьютерной информации

**Объектом исследования** является общественные отношения в сфере борьбы с преступлениями против компьютерной информации.

**Предметом исследования** являются нормы уголовного и иного законодательства, регулирующие отношения в сфере использования компьютерной информации, судебно-следственная практика по уголовным делам о преступлениях, предусмотренных гл. 28 УК РФ, теоретические положения, тенденции развития и совершенствования методов уголовно-правовой защиты информации, прав и законных интересов её обладателей.

**Цели и задачи исследования.** Целью настоящего исследования является исследование теоретических вопросов механизма уголовно-правовой защиты информации, прав и законных интересов её обладателей.

Для реализации указанной цели поставлены следующие **задачи:**

- изучить научные подходы к понятию составов преступлений, предусмотренных гл. 28 УК РФ и их соотношение с действующим законодательством РФ;

- исследовать правоприменительную практику при рассмотрении судами уголовных дел о преступлениях против компьютерной информации;

- обосновать значение понятийного аппарата в области законодательства и доктрины для правоприменительной практики;

- выявить недостатки правового регулирования рассматриваемых отношений;

- разработать рекомендации, направленные на повышение эффективности механизма уголовно-правовой защиты информации, прав и законных интересов её обладателей.

**Методология исследования**. В работе использованы исторический, сравнительно-правовой, системно-структурный и формально-логический методы исследования.

**Теоретическая база исследования.** Источниковой базой является, прежде всего, Конституция РФ и действующее уголовно законодательство России. В работе использованы труды таких ученых, как Абов А.И., Алескеров В.И., Айсанов Р.М., Батурин Ю.М., Бачило И.Л., Бойцов А.И., Бородин А.В., Бражник С.Д., Васильев Н.В., Волеводз А.Г., Воробьев В.В., Гаврилин Ю.В., Городов О.А., Дворецкий М.Ю., Золотухин С.Н., Копылов В.А., Ляпунов Ю.И., Медведовский И.Д., Мешков В.М., Панфилова Е.И., Пущин В.С., Евдокимов К.Н. и другие ученые.

Э**мпирическую базу исследования** представляют результаты обобщения уголовных дел, в том числе прекращенных в суде, как в Тюменской области, так и в других регионах РФ в период.

**Основные положения, выносимые на защиту:**

1. Несмотря на то, что информационная безопасность традиционно ассоциируется главным образом с компьютерными технологиями и совершаемыми в этой сфере правонарушениями, значительное количество

статей УК РФ направлено на защиту иных отношений, в которых использование компьютерной техники и информационных технологий не предполагается либо такое использование не является определяющим. Речь идет об обеспечении сохранности различных видов тайны (личной, государственной), обеспечении неприкосновенности частной жизни, а также чести и достоинства человека и гражданина, об обеспечении права на доступ к информации, права на комфортную информационную среду, не посягающую на мораль, нравственность, психологический комфорт личности.

2. С учетом теоретических подходов и сложившейся практики сформулированы основные, значимые для квалификации преступлений в сфере компьютерной информации понятия, такие как: неправомерный доступ, блокирование, уничтожение, копирование, модификация информации, вредоносная программа, технические средства, программные средства, средства хранения, обработки или передачи компьютерной информации и прочее.

3. Сделан вывод о том, что требуется на законодательном уровне разъяснить ряд вышеуказанных и других специальных понятий, в то время как диспозиции статей, предусмотренных гл. 28 УК РФ нецелесообразно еще больше нагружать специальной терминологией, так как это вызовет трудности в правоприменительной практике.

4. Преступления против компьютерной информации имеют свои специфические черты, которые оказывают существенное влияние на особенности криминальной, а также криминалистической деятельности. Такими чертами являются: место совершения преступления, носящее трансграничный характер, технологии, позволяющие в кратчайшие сроки «замести» следы преступления, терминологическая загруженность и прочее.

5. Преступления в сфере компьютерной информации зачастую граничат с преступлениями против собственности и иных направленностей, ввиду чего особую значимость приобретает установление направленности преступного умысла при их расследовании и рассмотрении судами.

**Научно-практическая значимость исследования.** В работе развиваются представления о понятии и предмете преступлений, направленных против компьютерной информации, содержащихся в гл. 28 УК РФ. Анализ сложившейся ситуации в соотношении доктрины и закона позволяет сформулировать ряд конкретных практических рекомендаций и предложений, направленных на повышение эффективности борьбы с преступностью в данном направлении.

**Апробация результатов исследования.** Основные положения магистерской диссертации были изложены в научной статье:

Косогоров Е.М. Компьютерные преступления как способ обеспечения различных тайн // Актуальные проблемы современного российского права: материалы X Международной научно-практической конференции. Невинномысск, 7-8 июня 2018 года. Невинномысск: НГГТИ, 2018. 368 с. (С.246-248; 0,25 п.л.)

**Структура работы**: работа состоит из введения, трех глав, заключения и библиографического списка.

# ГЛАВА 1. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

## 1.1. ОБЪЕКТИВНЫЕ ПРИЗНАКИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Для отграничения неправомерного доступа к компьютерной информации от других преступлений и правонарушений, определения характера и степени общественной опасности деяния, тяжести причиненного или возможного вреда, направленности преступного деяния необходимо установить и определить объект преступного посягательства. Установление объекта преступного посягательства может послужить программой для определения группы смежных составов, среди которых нужно будет уже более тщательно искать подходящую норму уголовного закона [80, с. 93].

Некоторые ученые определяют непосредственный объект преступления, предусмотренного ст. 272 УК РФ, через состояние защищенности, то есть как безопасность информационных систем, базирующихся на использовании ЭВМ, системе ЭВМ или их сети [22, с. 10; 78, с. 83], безопасность деятельности всех субъектов, являющихся обладателями информации или операторами информационных систем, по созданию или использованию информации, т.е. по реализации ими своих полномочий в пределах, установленных законом [27, с. 95], безопасность использования компьютерной информации, информационных ресурсов и систем [115, с. 346].

Однако есть и другие мнения ученых, которые относят к непосредственному объекту неправомерного доступа к компьютерной информации конкретные права и интересы по поводу её использования, например, право владельца системы на неприкосновенность информации, содержащейся в системе, конкретные права и интересы, охраняемые уголовным законом, подвергшиеся посягательству в результате совершения общественно опасного деяния, права на информацию её владельца либо третьих лиц,

охраняемые законом права и интересы общества, государства, физических и юридических лиц в сфере владения, распоряжения, пользования компьютерной информацией [52, с. 46; 64, с. 634, 640, 642; 56, с. 68].

Согласимся с мнением В.Г. Степанова-Егоянц о том, что не совсем верным представляется определение непосредственного объекта преступления, предусмотренного ст. 272 УК РФ, через ущерб какому-либо социальному благу и через состояние защищенности информации, так как в теории уголовного права данное преступление направлено на изменение общественных отношений, а не на причинение вреда социальному объекту и не на нарушение какого-либо состояния. Таким образом, под непосредственным объектом рассматриваемого преступления полагаем верным понимать общественные отношения, обеспечивающие право обладателя компьютерной информации на её безопасное создание, хранение, использование и передачу. Также целесообразно рассмотреть дополнительный объект неправомерного доступа, как общественные отношения, требующие отдельной защиты, так как при посягательстве на основной объект они неизбежно поставлены в опасность [140, с. 25]. Полагаем, что дополнительный объект придаёт рассматриваемому преступлению повышенную общественную опасность. К дополнительному объекту, в частности, могут относиться отношения в области авторского права, права собственности, неприкосновенности частной жизни и проч. Отметим, что при наличии дополнительного объекта при совершении преступления, предусмотренного ст. 272 УК РФ, квалификация деяния, как правило, даётся по совокупности с соответствующими нормами уголовного закона, например, если неправомерный доступ к компьютерной информации, её копирование либо распространение каким-либо образом касалось личной или семейной тайны потерпевшего, деяние будет квалифицировано по совокупности ст. 272 и ст. 137 УК РФ.

Что касается предмета неправомерного доступа к компьютерной информации, отметим, что единого подхода в научном мире к его определению нет и данный вопрос представляет большой научный интерес, в том числе,

разделяются мнения о том, всегда ли предметом преступления может быть объект материального мира. Так, многие отечественные ученые отрасли, предлагают понимать предмет как технические устройства, на которых хранится соответствующая информация, другие признают предметом любого компьютерного преступления должен считаться компьютер как информационная система либо носитель информации [100, с. 273-274]. Также существует схожая позиция, согласно которой предметом преступления является компьютерная информация, компьютер, компьютерная система или компьютерная сеть [41, с. 85-86]. В тоже время, многие ученые данный подход находят ошибочным, отмечая, что такой подход значительно затрудняет разграничение преступлений против компьютерной информации и преступлений против собственности, так как хищение либо уничтожение компьютера не может подлежать квалификации по ст. 272 УК РФ.

Вместе с тем, важно отметить, что в научных кругах развивается полемика касательно вопроса об определении информации «охраняемой законом», являющейся предметом преступления, в соответствии с диспозицией рассматриваемой статьи. Некоторые ученые полагают, что слова «охраняемой законом» и отнести к предмету вообще любую информацию, либо понимать под охраняемой любую информацию, представляющую ценность для собственника [142, с. 114]. Однако автор придерживается позиции Ю. Гульбина, о том что все же предметом преступления может выступить лишь охраняемая законом информация, однако, в тоже время не охраняемой информации практически не существует. При определении подхода к охраняемой законом информации отталкиваться следует от Федерального закона от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации», согласно положениям которого информация разделена на общедоступную и ограниченную. В соответствии со ст. 7 Закона «к общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен», тем самым закреплены основные её свойства, в тоже время, в соответствии с п. 3 ст. 3 Закона обладатель

наделяется правом ограничения доступа к информации, определять его условия и порядок. Таким образом, информация становится охраняемой в момент ограничения доступа к ней собственником, в то время как если таковые меры не приняты и информация остается общедоступной, какие-либо манипуляции с ней (доступ, копирование, распространение) не могут образовать состав преступления, предусмотренного ст. 272 УК РФ. Кроме того, автоматически подпадает под рассматриваемую норму информация, охраняемая законом в режиме тайны, в том числе государственная, банковская, тайна следствия и судопроизводства, персональные данные, конфиденциальная информация, служебная тайна (данная статья исключена из ГК РФ, однако сведения по прежнему охраняются), врачебная тайна, нотариальная тайна, тайна личной жизни, адвокатская тайна, тайна переписки, телефонных переговоров и почтовых отправлений, коммерческая тайна, интеллектуальная собственность. Отметим, что согласно законодательству РФ на сегодняшний день насчитывается порядка сорока видов тайн.

Не менее спорным в научных кругах является вопрос о возможности отнесения информации к категории собственности, так как на законодательном уровне понятие «собственник информации» не закреплено, однако отметим, что диспозиция исследуемой статьи предусматривает посягательство именно на компьютерную информацию, а не на её материальный носитель как объект собственности. Вместе с тем Федеральный закон «Об информации, информационных технологиях и защите информации» в ч. 5 ст. 2 определяет понятие обладателя информации как «лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам». Отметим, что суды при принятии решения по уголовному делу устанавливают был ли ограничен доступ к соответствующей информации и охраняется ли она законом.

Например, в 2012 году, Ленинским районным судом г. Тюмени в отношении Г. вынесен приговор по ч. 1 ст. 272 УК РФ, судом установлено, что

Г., достоверно зная, что данные, необходимые для подключения к установленному интернет-сайту (логин, пароль) дают возможность доступа к информации, доступ к которой в соответствии с ФЗ «Об информации, информационных технологиях и защите информации» ограничен и может быть получен только лицами, которые на законных основаниях получили вышеуказанные данные (логин и пароль), совершил неправомерный доступ к компьютерной информации [156].

Также отметим, что в судебных решениях можно встретить использование судами терминов «собственник информации», «владелец информации», несмотря на то, что с вступлением в силу Федерального закона «Об информации, информационных технологиях и защите информации» в 2006 году, данные понятия были упразднены, и заменены одним – «обладатель информации», определение которому давалось выше. Однако в некоторых нормативных документах и по сей день можно встретить применение категории «собственник» к информации. Например, ГОСТ Р 50922-2006 (Утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 27.12.2006 № 373-ст) «Защита информации. Основные термины и определения» в п. 2.5.2 мы встречаем положения об информации, являющейся «предметом собственности» [13].

Кроме того, некоторыми авторами высказываются мнения об обязательной ценности информации, на которую совершено посягательство, определяя данную категорию как «максимальную пользу, которую может принести данная информация либо максимальные потери, к которым приведёт её утрата» [82, с. 101]. Однако на законодательном уровне критерия определения ценности информации не закреплено, и также с учетом того, что ценность может варьироваться в зависимости от самого её обладателя, автор полагает, что такой критерий как «ценность» не должен быть составообразующим для данного преступления, а определяться самим её обладателем в рамках конкретной ситуации.

Переходя к исследованию объективной стороны состава рассматриваемого преступления, сразу отметим, что и этот вопрос является в науке дискуссионным. Судебно-следственная практика сталкивается с трудностями и ошибками в квалификации преступлений, предусмотренных ст. 272 УК РФ, прежде всего из отсутствия единого подхода, в отечественной науке, к самому понятию «неправомерный доступ к охраняемой законом компьютерной информации». Согласимся с мнением А.Г. Волеводза о том, что «доступ всегда связан с совершением определенных действий» [36, с. 66], и весьма маловероятно, что объективная сторона данного преступления может выразиться в бездействии, позволившем получить субъекту преступления неправомерный доступ к компьютерной информации. А.В. Сизов дает техническое определение доступа к компьютерной информации как «возможность ознакомления, копирования, уничтожения и модификации информации, полученная вследствие несанкционированного преодоления программной, аппаратной или комплексной» Федеральный закон «Об информации, информационных технологиях и защите информации» даёт нам определение доступа как «возможность получения информации и её использования», также раскрывая понятие «использование информации» как распространение по своему усмотрению, то есть осуществление действий, направленных на получение информации неопределенным кругом лиц или её передачу неопределенному кругу лиц.

Отечественные юристы видят предложенное законодательством определение «доступ» находят проблематичным и спорным, которое должно применяться к уголовному закону с оговоркой, так как является слишком широким, в то время как доступ, согласно диспозиции ст. 272 УК РФ должен быть «фактом», активным действием, сегодняшнее законодательное его толкование как «возможность» подразумевает не только фактическое овладение и информацией, но и право на доступ к ней [139, с. 41]. Не смотря на то, что состав преступления материальный и председатель ВС РФ в своём комментарии к уголовному кодексу придерживается позиции, что состав

преступления образует именно наступления возможности обладания информацией, автору данная позиция видится верной по аналогии с тайным хищением чужого имущества.

При определении подхода к неправомерности доступа к компьютерной информации, как обязательному признаку состава рассматриваемого преступления автором также отмечено многообразие позиций ученых на этот счёт. По мнению М.М. Смирнова и А.П. Толмачева доступ является неправомерным в случае, «если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации» [136, с. 177], однако автор склонен согласиться с мнением Степанова-Егиянц о том, что неправомерность доступа не должна находиться в исключительной зависимости от последствий, указанных в диспозиции статьи. Разные ученые высказывают мнения о том, что неправомерность доступа складывается из отсутствия согласия обладателя информации на ознакомление с ней, на распоряжение ею, нарушение порядка доступа к информации, установленного её обладателем [68, с. 653]. Кроме того высказываются мнения о том, что информация обязательно должна быть защищена определённым образом, а в противном случае такой доступ не будет считаться преступным.

С учетом существующих доктринальных положений автор приходит к выводу о том, что под неправомерностью доступа следует понимать такой доступ, при котором действия, направленные на получение возможности использования компьютерной информации тем или иным образом, осуществлены против воли обладателя компьютерной информации, либо с нарушением порядка доступа, установленного обладателем. Аналогичная же позиция вытекает из судебной практики, при принятии судами решений в различных регионах и на различных уровнях. В целом можно отметить, что судебная практика вполне согласуется с положениями доктрины.

Автор считает необходимым также коротко подвести о том, что не образует состава рассматриваемого преступления, именно ввиду отсутствия объективной стороны. Как уже прослеживается из текста настоящей работы, в

рамках рассмотрения предмета преступления, обычное хищение или иным путем завладение техническими средствами (в том числе компьютером) хранения, обработки компьютерной информации, а также уничтожение такой информации путём механического повреждения, непроизвольный доступ вследствие ошибки, не образует состава неправомерного доступа к компьютерной информации [36, с. 66]. При этом отметим, что ряд авторов относительно механического повреждения информации считают, что квалификацию необходимо давать в зависимости от направленности умысла виновного, так как если уничтожение совершенно именно с целью повреждения компьютерной информации, содеяно должно быть квалифицировано по совокупности ст. 167 и ст. 272 УК РФ [61, с. 146]. По тем же соображениям К.Н. Евдокимов считает целесообразным введение в УК РФ ст. 272.1 «Незаконное завладение ЭВМ или иным машинным носителем компьютерной информации без цели хищения для осуществления неправомерного доступа к компьютерной информации» [56, с. 53].

Далее необходимо рассмотреть последствия совершения рассматриваемого преступления, которые указаны в ч. 1 ст. 272 УК РФ, однако на законодательном уровне их понятие не раскрыто, что также вызывает трудности в судебно-следственной практике. Наиболее опасным, по мнению автора, последствием является именно уничтожение информации, так как оно несёт невосполнимый вред, соответственно наиболее существенный. В доктрине на сегодняшний день сложилось понятие уничтожения, которое подразумевает удаление информации при невозможности восстановления либо при наличии таковой, приведение информации в состояние абсолютной невозможности её дальнейшего использования [103, с. 55-56]. В случае, если уничтоженная (удаленная) информация существует не в единственном экземпляре и беспрепятственно может быть восстановлена, содеянное должно квалифицироваться по ч. 3 ст. 30 УК РФ, как покушение, так общественно-опасные последствия в данном случае не наступают вопреки воле виновного и по независящим от него обстоятельствам. Многие авторы высказывают мнение

о том, что при таких обстоятельствах данное деяние не образует состава преступления, так как не достигает уровня общественной опасности, присущего преступлению [29, с. 80], однако с данным мнением сложно согласиться, ввиду его несогласованности с принципами уголовного закона.

Что касается момента наступления последствия, В.М. Мешков говорил о следующем: "наступление преступных последствий будет налицо с того момента, когда файл или его часть станут "невидимыми" для средств программного обеспечения, используемого законным пользователем, и недоступными для их стандартных команд" [94, с. 60]. Также отметим, что изменения, не влияющие качественные характеристики информации (например, переименование файла или его перемещение) не могут считаться её уничтожением [94, с. 60].

Следующим последствием, наступление которого предусматривает изучаемая норма это блокирование компьютерной информации. К определению данного понятия в доктрине также имеется не один подход, однако в большинстве ученые при его определении отталкиваются от момента возможности либо невозможности пользоваться такой информацией. А.Л. Осипенко связывает блокирование как ограничение доступа компьютерной информации, с определенным временным промежутком и фактом сохранности такой информации в системе хранения [103, с. 56]. По мнению В.М. Мешкова блокирование связано не только с невозможностью доступа к информации, но и на его существенное затруднение, опять же признавая необходимость сохранности информации [94, с. 60], Ю. Ляпунов и В. Максимов отмечают при определении невозможность доступа к информации именно законным её обладателем [84, с. 9]. Обращаясь к субедно-следственной практике отметим, что судами зачастую используется ГОСТ Р 53114-2008 "Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения", согласно которому "блокирование доступа (к информации): прекращение или затруднение доступа к информации лиц, имеющих на это право (законных пользователей)".

Среди ученых расходятся мнения о том, на протяжении какого времени должна продолжаться блокировка компьютерной информации, чтобы такое деяние приобрело уровень общественной опасности, подпадая под норму уголовного закона, так, А.Н. Ягудин считает, что уголовная ответственность должна наступать независимо от продолжительности блокирования и наступивших последствий, а Д. Савельева занимает противоположную позицию, согласно которой блокирование должно признаваться преступным продолжаясь на протяжении того времени в течение которого становится возможным нарушение нормальной работы обладателя компьютерной информации (пользователя). Ленинский районный суд г. Тюмени при рассмотрении ранее уже указанного уголовного дела в отношении Г. в описании преступного деяния сослался на временной промежуток менее двух минут (65 секунд). Автор работы считает необходимым согласиться с мнением Д. Савельевой, преступная длительность блокирования должна определяться с учетом конкретной ситуации и факта нарушения нормальной работы обладателя информации, а основным признаком данного последствия должна являться невозможность доступа, но не временной промежуток.

Модификация компьютерной информации. В теории уголовного права можно найти множество определений понятия "модификация":

- изменение первоначальной информации без согласия собственника или иного законного владельца;

- изменение (переработка) исходного состояния, осуществляемое без согласия законного владельца;

- внесение в информацию изменений, не санкционированных обладателем;

- изменение содержания информации по сравнению с той информацией, которая первоначально (до совершения деяния) была в распоряжении собственника или законного пользователя;

- видоизменение информации, характеризующееся появлением новых (очевидно, нежелательных) свойств;

- любые изменения компьютерной информации.

С. Кочои и Д. Савельев утверждают, что модификация может осуществляться как путем частичной замены первоначальной информации на другую, так и добавлением новой информации к первоначальной. По мнению этих авторов, с которыми трудно не согласиться, модификацией является изменение первоначального вида предоставления информации, например: перестановка абзацев, строк, страниц, включение посторонних элементов, нарушение порядка расположения в базе данных; - изменение первоначального состояния информации (например, реструктурирование или реорганизация базы данных, удаление или добавление записей, содержащихся в ее файлах, перевод программы для ЭВМ или базы данных с одного языка на другой), не меняющее сущность объекта; - внесение изменений в компьютерную информацию, которые существенно отличают ее от изначальной; - внесение в нее любых изменений, кроме связанных с адаптацией программ для ЭВМ или базы данных.

Согласно подп. 9 п. 2 ст. 1270 ГК РФ адаптация программы для ЭВМ или базы данных "это внесение изменений, осуществляемое исключительно в целях обеспечения функционирования программы для ЭВМ или базы данных на конкретных технических средствах пользователя или под управлением конкретных программ пользователя". Такого рода изменения носят технический характер и не препятствуют использованию компьютерной информации ее владельцем.

Гражданский кодекс РФ в подп. 9 п. 2 ст. 1270 ГК РФ под модификацией понимает любые изменения программы для ЭВМ, в том числе перевод такой программы или базы данных с одного языка на другой. При этом мы разделяем мнение И.А. Сало, считающей, что "переносить термин "модификация", предназначенный для отношений, связанных с правовой охраной результатов интеллектуальной собственности, на отношения, возникающие при обеспечении защиты информации... является необоснованным". На наш взгляд, применять толкование понятия "модификация авторского права" для раскрытия

содержания понятия "модификация", применимого в ст. 272 УК РФ, не вполне допустимо, так как объекты при нарушении авторских прав и при совершении преступлений в сфере компьютерной информации различны.

Как считает В.С. Пущин, ведущей составляющей в термине "модификация" является "направленность изменения информации". Направление должно быть желаемым (заданным) виновным. Если нет направленности в выполняемых действиях, то это уже не модификация, а уничтожение. Аналогичного мнения придерживается и И.А. Сало. Анализ судебных постановлений позволяет сделать вывод, что суды в основном толкуют понятие "модификация" как изменение информации. Приведем в качестве примера приговор Новочеркасского городского суда Ростовской области от 10 апреля 2013 г. в отношении Б., которая, реализуя свой преступный умысел, направленный на совершение неправомерного доступа к охраняемой законом компьютерной информации - автоматизированной информационной системе и ее модификацию, чтобы занизить кадастровую стоимость земельного участка, завладела информацией о доменной учетной записи и пароле доступа В.Л.В. к автоматизированной системе.

В целях сокрытия планируемого преступления, осознавая отсутствие в указанное время на рабочем месте иных сотрудников кабинета, Б. в отсутствие иных сотрудников и в нарушение инструкции по организации парольной защиты автоматизированной системы включила служебную систему В.Л.В. и в результате введения наименования доменной учетной записи В.Л.В. умышленно совершила неправомерный доступ к охраняемой ст. 14 ФЗ "Об информации, информационных технологиях и о защите информации" компьютерной информации, размещенной на сервере, установленном в кабинете того же здания. Осуществив неправомерный доступ, Б. в нарушение ст. 16 Федерального закона от 24 июля 2007 г. № 221-ФЗ "О государственном кадастре недвижимости", а именно в отсутствие документа для учета изменений, внесла изменения в сведения о кадастровой стоимости с показателя 196 829 263 руб. 26 коп. на показатель 35 596 240 руб. 9 коп. земельного

участка с кадастровым номером (данные изъяты) и значения удельного показателя кадастровой стоимости в размере "2383,73 рублей за кв. метр", чем модифицировала ее. Совершив указанные действия, Б. выключила компьютер В.Л.В., продолжив заниматься личными делами. Как видно из приведенного выше приговора, суд признал в качестве последствия неправомерного доступа к компьютерной информации изменение сведений о кадастровой стоимости земельного участка [160].

Отсутствие сформированной единообразной судебной практики и единого толкования у правоприменителей положений ст. 272 УК РФ приводит к неоднозначному толкованию норм указанного Кодекса. Так, суды по-разному определяют вид общественно опасных последствий, наступающих при замене обвиняемым фотографий одного лица на фотографии другого лица, размещенные на электронных страницах потерпевших в социальных сетях.

Так, судья Ленинского районного суда г. Пензы в приговоре от 22 ноября 2010 г. по уголовному делу № 1-188/10 установил, что 24 апреля 2010 г. Б. из личных неприязненных отношений к В. осуществил неправомерный доступ к охраняемой законом компьютерной информации - содержимому принадлежащей В. личной электронной страницы, удалил личную переписку В., что повлекло уничтожение защищаемой законом информации, а также заменил главную фотографию (аватар), принадлежащую В., на фотографию другого лица, что повлекло модификацию защищаемой законом информации [151].

Каменский городской суд Пензенской области в приговоре от 11 апреля 2011 г. по уголовному делу № 1-51/2011 установил, что действия обвиняемого М., аналогичные действиям, описанным в предыдущем приговоре, привели к наступлению общественно опасных последствий в виде уничтожения компьютерной информации. Подсудимый М. обвинялся в совершении двух неправомерных доступов к компьютерной информации. Используя незаконно полученный пароль и логин для доступа к почтовому ящику А., М. без ведома законного пользователя осуществил неправомерный доступ к персональной

странице А., расположенной на сервере "Вконтакте", после чего произвел замену главной фотографии А. на фотографию лошади. Действия М. по неправомерному удалению фотографии и замене фотографии на персональной странице А. суд квалифицировал по ч. 1 ст. 272 УК РФ как неправомерный доступ к охраняемой законом компьютерной информации, при этом деяние повлекло уничтожение информации [155].

На наш взгляд, описанные выше деяния приводят к наступлению общественно опасных последствий в виде модификации, т.е. изменения первоначальной информации. Безусловно, если бы фотографии удалялись виновными с личных страниц потерпевших без замены на другие изображения, то наступили бы общественно опасные последствия в виде уничтожения компьютерной информации.

Серьезные прения в уголовно-правовой науке касаются квалификации незаконного подключения к сети Интернет при помощи чужих пользовательских паролей и логинов. В России сложилась устойчивая практика, когда такие деяния квалифицируются судами по ст. 272 УК РФ. Суды в приговорах указывают, что "учетно-регистрационные данные - логин и пароль... правомерно могут использоваться только лицом, их получившим на законных основаниях" [156], "введение учетных реквизитов другого лица без ведома последнего" [150] является неправомерным доступом к компьютерной информации, при этом "указанные действия влекут изменения статистической информации на серверах провайдера об объеме услуг, предоставляемых лицу, которому принадлежат реквизиты, а также искусственные затруднения доступа законного пользователя к ресурсам сети, так как работу в сети Интернет в одно и то же время с одним и тем же паролем может осуществлять лишь один пользователь, то есть модификацию и блокирование компьютерной информации". Такие деяния в правоприменительной практике квалифицируются по совокупности преступлений, предусмотренных ст. 272 и 165 УК РФ.

По мнению А.Л. Осипенко, "фиксируемые в базах данных провайдера

сведения о неправомерных сеансах доступа лица в Интернет не могут считаться фактами неправомерной модификации содержащейся в них информации", потому что "происходящая при этом модификация учетно-статистической базы данных не связана с умыслом".

В уголовно-правовой науке существует еще одно мнение, в соответствии с которым доступ к сети Интернет с использованием чужих учетно-регистрационных данных нельзя считать неправомерным и квалифицировать по ст. 272 УК РФ, "так как подавляющее большинство информации в этой сети носит открытый характер и она не запрещена к копированию, а уголовный закон запрещает неправомерный доступ только к охраняемой законом информации". В.В. Воробьев считает, что нельзя квалифицировать такие действия по ст. 272 УК РФ, если "правоохранительными органами не был установлен факт доступа виновным к охраняемой законом информации" [37, с. 66].

Противоположного взгляда придерживается М.В. Старичков, считающий доступ к компьютерной информации с использованием чужого имени и пароля неправомерным. По мнению ученого, "во время доступа в Интернет на сервере, принадлежащем провайдеру, происходит модификация сведений о времени работы и о состоянии счета владельца учетного имени. Кроме того, на период подключения нарушителя блокируется доступ добросовестному пользователю, поскольку одновременная работа в сети двух компьютеров под одним и тем же учетным именем технически недопустима".

Мы считаем, что доступ в Интернет описанным выше способом, без всякого сомнения, является неправомерным. Изменение статистических данных провайдера является модификацией компьютерной информации и охватывается косвенным умыслом виновного. Кроме того, регистрационные данные признаются информацией, охраняемой законом, и этого достаточно для квалификации доступа по ст. 272 УК РФ. Также следует отметить, что выход в сеть с чужими регистрационными данными всегда блокирует возможность одновременного доступа к компьютерной информации ее законного

обладателя. Квалификация правоохранительными и судебными органами доступа к компьютерной информации с использованием чужих регистрационных данных по ст. 272 УК РФ является верной.

Вопрос о том, следует ли считать незаконное получение чужих регистрационных данных для доступа в сеть Интернет сбором сведений, составляющих коммерческую тайну, и необходима ли в таких случаях дополнительная квалификация по ч. 1 ст. 183 УК РФ, считается в правовой науке дискуссионным.

По мнению А.Н. Ягудина, "нормы ст. 183 УК РФ должны применяться, если виновный, имея умысел на собирание сведений, составляющих коммерческую тайну, при помощи незаконно полученных реквизитов доступа осуществляет копирование информации (баз данных, служебной документации и т.п.) с внутренней локальной сети коммерческой организации" [142, с. 102].

Проведенный анализ практики показывает, что следственные органы и суды использование виновным для доступа в сети Интернет чужих логина и пароля обычно квалифицируют по совокупности ст. 272 и 165 УК РФ, не используя при этом ст. 183 УК РФ. Автор полностью поддерживает М.В. Старичкова, утверждающего, что по делам указанной категории вменение ст. 183 УК РФ не только оправданно, но и необходимо, поскольку целью ст. 272 УК РФ является уголовно-правовая охрана общественных отношений, связанных с безопасным использованием компьютерной информации, а целью ст. 183 УК РФ - связанных с безопасным осуществлением экономической деятельности.

Приведенные выше примеры из судебной практики подтверждают отсутствие единообразия в судебно-следственной практике при квалификации неправомерного доступа к охраняемой законом компьютерной информации.

Копирование компьютерной информации. В настоящее время сложилось несколько подходов к решению вопросов о том, что такое копирование компьютерной информации и какие способы ее копирования существуют. Проведенный анализ следственно-судебной практики позволил нам сделать

вывод, что суды определяют "копирование компьютерной информации" как перенос с одного носителя информации на другой.

В отечественной правовой науке к числу дискуссионных относится вопрос, является ли автоматическое копирование информации в оперативно-запоминающее устройство компьютера копированием информации, т.е. общественно опасным последствием неправомерного доступа к компьютерной информации, установление наличия которого считается необходимым условием привлечения виновного к ответственности по ст. 272 УК РФ.

В.В. Крылов высказывает следующую точку зрения: "Не следует признавать справедливым утверждение о том, что нельзя инкриминировать лицу копирование информации в случае, когда в ходе проникновения в ЭВМ и ознакомления с находящейся там информацией программные механизмы ЭВМ автоматически копируют тот или иной файл" [78, с. 103].

Противоположного мнения придерживается А.Г. Волеводз, отмечая, что лицу, осуществившему доступ к компьютерной информации для ознакомления с ней, не может инкриминироваться в вину ее копирование, обусловленное не зависящим от его воли автоматическим действием аппаратно-программных средств правомерного пользователя. С.В. Озерский, Ю.Н. Лазарев, А.Ю. Лавров считают, что "копирование, обусловленное автоматическим действием программных средств правомерного пользователя (например, в операционной системе UNIX действуют программы-"демоны", которые с заданной периодичностью осуществляют контроль работоспособности системы, сохраняя критическую системную информацию путем ее дублирования), не может вменяться в вину лицу, осуществившему доступ к компьютерной информации для ознакомления, как копирование".

Копирование информации на самом оригинальном носителе (например, в дисковой памяти компьютера организуются несколько файлов одного и того же содержания) или на однородном носителе, оставшемся в распоряжении пользователя (например, копия делается в памяти компьютера, образующей с данным компьютером систему), А.Ю. Карманов определяет как размножение

информации. Мы считаем, что на практике может возникнуть ситуация копирования информации на одном и том же носителе информации. Например, на одном компьютере существуют папки нескольких локальных пользователей. Если один локальный пользователь, имея преступный умысел на копирование информации из папки другого локального пользователя в свою, осуществил неправомерный доступ к охраняемой законом компьютерной информации, скопировал ее в свою папку, то он подлежит привлечению к уголовной ответственности по ст. 272 УК РФ, несмотря на то, что информация осталась на том же носителе информации.

В процессе правоприменения возник вопрос о том, какие способы копирования образуют состав исследуемого преступления. Копирование может осуществляться не только переносом на другой машинный носитель, но и переписыванием, фотографированием с экрана компьютера. По мнению одних ученых, копирование компьютерной информации может быть осуществлено путем записи содержащегося во внутренней памяти ЭВМ файла на дискету, его распечатки и т.п. Копирование компьютерной информации от руки путем фотографирования текста с экрана дисплея, а также считывание информации путем перехвата излучений ЭВМ, расшифровки шумов принтера и пр. не образуют состава преступления в рамках данной статьи УК РФ.

В перечисленных выше случаях квалификация должна осуществляться по другим статьям УК (например, ст. 183 УК РФ). Такая же точка зрения сформировалась у Н.А. Борчевой, которая считает, что "сущность копирования заключается в переносе информации с одного машинного носителя на другой машинный носитель, а также неправомерной записи компьютерной информации в память ЭВМ. Другие способы копирования (фотографирование информации с монитора, распечатка и пр.) не образуют состава преступления" [28, с. 8].

В юридической науке существует и более широкий подход к определению копирования компьютерной информации. А.С. Попов, Е.А. Панфилова утверждают, что "копирование компьютерной информации - это

воспроизведение информации в любой материальной форме". В связи с этим нельзя согласиться с утверждением, что копирование компьютерной информации от руки путем фотографирования с экрана дисплея не является наказуемым по ст. 272 УК РФ [106, с. 15]. Такой вывод исследователи основывают на том, что в статье не говорится о способах копирования, а фотографии есть доказательство неправомерного доступа к компьютерной информации. Его последствием, по мнению приверженцев широкого подхода, является и несанкционированное копирование охраняемой законом компьютерной информации с экземпляра распечатки принтера (листинга). Копирование - это воспроизведение информации в любой материальной форме [106, с. 26].

Трудно не согласиться с позицией В.С. Пущина, что "копированием не будет признаваться ознакомление со структурой сети или файловой системы на каком-либо носителе (структура директорий, списки файлов, содержащихся в конкретных директориях), т.к. подобного рода сведения нельзя подвести под какую-либо категорию охраняемой законом информации" [109, с. 52]. С.Ю. Бытко отмечает, что "широкое толкование неоправданно увеличивает сферу действия преступлений, предусмотренных гл. 28 УК РФ" [34, с. 31].

Проведенный анализ судебных дел, связанных с привлечением виновных к ответственности за неправомерный доступ к компьютерной информации, позволяет сделать вывод, что суды не всегда правильно понимают понятия "доступ" и "последствия", отождествляя их, что приводит к ошибкам в толковании норм Уголовного кодекса РФ.

Далее остановимся на рассмотрении существующих в науке предложений по модернизации положений ст. 272 УК РФ, касающихся последствий неправомерного доступа к компьютерной информации.

Существенным недостатком гл. 28 УК РФ в целом и ст. 272 УК РФ в частности С.Д. Бражник считает следующее: "Введение в оборот неопределенных в правовом отношении терминов (например: "уничтожение", "копирование", "блокирование", "модификация"...) без их легального

толкования вызывало бы серьезные трудности для правоприменителя" [30, с. 78-79]. Если при разном толковании одного и того же законодательного термина рамки (границы) криминализации оказываются подвижными и сужаются или, наоборот, расширяются, то применение таких терминов в уголовном законе недопустимо [83, с. 44].

С такой позицией ученых автор совершенно согласен, поскольку перегруженность диспозиции ст. 272 УК РФ техническими терминами и отсутствие их официального толкования привели к формированию множества взглядов и подходов к пониманию сущности видов последствий неправомерного доступа к компьютерной информации, а применение закона часто зависит от усмотрения правоприменителя.

Большинство правоведов недоработкой законодателя считают отсутствие в нормах УК РФ указания на "ознакомление с компьютерной информацией" как на общественно опасное последствие неправомерного доступа к компьютерной информации. Мы считаем такой взгляд справедливым и заслуживающим внимания со стороны законодателя. Действующая формулировка состава преступления, предусмотренного ч. 1 ст. 272 УК РФ, как материального исключает ряд ситуаций, когда указанных в законе последствий не наступает, но сам факт того, что информация становится известна третьему лицу, причиняет существенный вред ее обладателю.

Получается, что если информация была скопирована, то все признаки состава преступления есть, а если она была просто прочитана - нет [130, с. 188]. Ознакомление с информацией путем ее прочтения не менее опасно, чем ее копирование. В некоторых случаях злоумышленнику достаточно увидеть и прочитать информацию, и она теряет свою ценность или может быть применена им в дальнейшем без всякого копирования [130, с. 188]. Независимо от того, наступили ли указанные последствия или нет, сам по себе факт неправомерного доступа уже представляет собой грубейшее нарушение прав собственника на владение компьютерной информацией [90, с. 87].

А.Н. Ягудин предлагает "дополнить ст. 272.1 УК РФ,

предусматривающую ответственность за неправомерный доступ к компьютерной информации, повлекший полное либо частичное ознакомление с ней" [142, с. 9]. А.Л. Осипенко рекомендует ввести "несанкционированное собственником ознакомление лица с защищаемой законом информацией".

А.В. Суслопаров видит решение создавшейся проблемы в том, чтобы оставить указание на копирование информации, убрав уничтожение, блокирование или модификацию. Такое предложение ученый обосновывает тем, что "без копирования информации сам факт незаконного доступа в нынешних российских условиях не обладает большой общественной опасностью". На его взгляд, отсутствие в уголовном законе понятия "блокирование" "позволит сделать УК РФ в этой части более понятным, лаконичным и соответствующим международно-правовым тенденциям борьбы с компьютерными преступлениями".

Некоторые ученые считают целесообразным ввести новые составы преступлений в гл. 28 УК РФ. В.С. Карпов предлагает "выделить в качестве самостоятельных составов преступлений такие способы совершения компьютерных преступлений, как несанкционированный доступ к компьютерной информации (ст. 272.1 УК РФ), неправомерное завладение компьютерной информацией (ст. 272.2 УК РФ), модификация компьютерной информации (ст. 272.3 УК РФ), изготовление и сбыт специальных средств для несанкционированного доступа к компьютерной системе или сети (ст. 272.4)" [41, с. 122]. Ученый советует в диспозициях статей "дать определение каждого способа, что упростит работу правоохранительных органов, кроме этого упростится деятельность правоприменителя в части квалификации деяния".

Автор не разделяет такой подход и считает, что выделение способов и последствий неправомерного доступа в отдельные статьи УК РФ приведет к неоправданной терминологической перегруженности гл. 28 УК РФ.

Для привлечения лица к ответственности за неправомерный доступ к компьютерной информации необходимо установить наличие причинной связи между действиями виновного лица и вредными последствиями, указанными в

диспозиции ст. 272 УК РФ. Д.Г. Малышенко называет необходимость установления причинной связи между действием и наступившими последствиями ахиллесовой пятой ст. 272 УК РФ, поскольку возможности вычислительной техники дают в руки преступника множество способов замести следы преступления в течение чрезвычайно малого промежутка времени [90, с. 67].

А.Е. Шарков отмечает, что неправомерный доступ к охраняемой законом компьютерной информации без наступления указанных в диспозиции последствий исключает правовое основание для привлечения лица к уголовной ответственности. Ученый предлагает исключить из диспозиции ч. 1 ст. 272 УК РФ указание на необходимость наступления последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации. Перечисленные последствия должны повлечь более строгую ответственность и могут быть сформулированы в качестве отягчающих обстоятельств.

Автор не разделяет подобных взглядов и полагает, что состав ст. 272 УК РФ должен остаться материальным, т.е. следует требовать установления факта наступления одного из перечисленных последствий для квалификации.

Проанализируем факультативные признаки неправомерного доступа к охраняемой законом компьютерной информации. Начнем со способов совершения преступления, предусмотренного ст. 272 УК РФ. Способы неправомерного доступа к охраняемой законом компьютерной информации, т.е. совокупность приемов и методов, используемых виновным для совершения данного преступления, могут быть самыми разными [142, с. 46].

Способы осуществления доступа: использование чужого имени, изменение физического адреса технического устройства, подбор пароля, нахождение и использование "пробелов" в программе, любой другой обман системы защиты информации. А.Г. Волеводз под способами понимает "использование специальных технических или аппаратно-программных средств, позволяющих преодолеть установленные системы защиты; незаконное использование действующих паролей и кодов для проникновения в компьютер

либо совершение иных действий в целях проникновения в систему или сеть под видом законного пользователя; хищение носителей информации при условии, что были приняты меры к их охране, если это деяние повлекло уничтожение или блокирование информации" [36, с. 36].

В.И. Струков, характеризуя методы несанкционированного доступа и перехвата компьютерной информации, использует следующую специфическую терминологию:

- "жучок" (buggi№g) - характеризует установку микрофона в компьютере с целью перехвата разговоров обслуживающего персонала;

- "откачивание данных" (data leakage) - отражает возможность сбора информации, необходимой для получения основных данных, в частности о технологии ее прохождения в системе;

- "уборка мусора" (scave№i№g) - характеризует поиск данных, оставленных пользователем после работы на компьютере. Этот способ имеет две разновидности - физическую и электронную. В физическом варианте он может сводиться к осмотру мусорных корзин и сбору брошенных в них распечаток, деловой переписки и т.п. Электронный вариант требует исследования данных, оставленных в памяти машины;

- метод следования "за дураком" (piggbacki№g) - характеризует несанкционированное проникновение как в пространственные, так и в электронные закрытые зоны. Его суть состоит в следующем. Если взять в руки различные предметы, связанные с работой на компьютере, и прохаживаться с деловым видом около запертой двери, где находится терминал, то, дождавшись законного пользователя, можно пройти в дверь помещения вместе с ним;

- метод "поиск бреши" (trapdoore№try) - используются ошибки или неудачи в логике построения программы. Обнаруженные бреши могут эксплуатироваться неоднократно;

- метод "мистификация" (spoofi№g) - используется при случайном подключении "чужой" системы. Злоумышленник, формируя правдоподобные отклики, может поддерживать заблуждение ошибочно подключившегося

пользователя в течение какого-то промежутка времени и получать полезную для него информацию, например коды пользователя [123, с. 14-15].

Рассмотрев объективные признаки неправомерного доступа к компьютерной информации, перейдем к исследованию его субъективных признаков.

## 1.2. СУБЪЕКТИВНЫЕ ПРИЗНАКИ НЕПРАВОМЕРНОГО ДОСТУПА К КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

Анализ диспозиции ст. 272 УК РФ позволяет сделать вывод о существовании следующих категорий субъектов неправомерного доступа к охраняемой законом компьютерной информации: общий субъект и специальный субъект.

Согласно положениям доктрины и уголовного закона, общим субъектом является вменяемой физическое лицо, достигшее шестнадцатилетнего возраста.

В настоящее время все больше ученых считают необходимым снизить возраст уголовной ответственности за совершение преступления, предусмотренного ст. 272 УК РФ, до 14 лет в связи с тем, что несовершеннолетние младше 16 лет зачастую обладают большими навыками работы на компьютере, чем взрослые люди, и вполне могут не только осознавать общественную опасность своих действий, но и предвидеть наступление тяжких последствий неправомерного доступа [21, с. 105; 90, с. 20].

Однако автор разделяет позицию тех ученых, которые считают возраст 16 лет оптимальным возрастом уголовной ответственности за совершение неправомерного доступа к охраняемой законом компьютерной информации. Так, например, И.А. Сало рассматривает предложение по снижению возраста уголовной ответственности за анализируемое преступление как не вполне обоснованное и негуманное.

Под специальным субъектом исследуемого преступления следует понимать лицо, совершившее неправомерный доступ к компьютерной

информации с использованием своего служебного положения.

В отечественной уголовно-правовой науке существуют два направления при определении такого признака специального субъекта, как использование служебного положения. Условно их определяют как широкий и узкий подходы. Приверженцы узкого подхода понимают под специальным субъектом преступления, предусмотренного ч. 2 ст. 272 УК РФ, по признаку совершения преступления лицом с использованием своего служебного положения: должностных лиц, государственных служащих и служащих органов местного самоуправления, не являющихся должностными, лиц, выполняющих управленческие функции в коммерческой или иной организации. Другими словами, специальным субъектом признаются лица, перечень которых содержится в ст. 201 и 285 УК РФ; лица, действующие противоправно в пределах служебной компетенции, в рамках предоставленных прав и полномочий. [63, с. 25].

Сторонником узкого подхода является Р.М. Айсанов, считающий, что "использование служебного положения означает, что лицо получает доступ к компьютерной информации незаконно, используя права, предоставленные исключительно в силу выполняемой служебной деятельности" [21, с. 109].

С.А. Пашин считает, что "под использованием служебного положения здесь понимается использование возможности доступа к ЭВМ, возникшей в результате выполняемой работы (по трудовому, гражданско-правовому договору), или влияния по службе на лиц, имеющих такой доступ. В данном случае субъектом преступления необязательно является должностное лицо" [68, с. 735].

Изучение приговоров позволяет сделать вывод, что суды при квалификации преступлений, предусмотренных ч. 2 ст. 272 УК РФ, понимают признак "использование служебного положения" с учетом широкого его толкования в отечественной юридической науке. По мнению большинства ученых, служебное положение дает возможность совершить неправомерный доступ к компьютерной информации тогда, когда "действия находятся в

пределах его служебной компетенции, хотя и совершаются с явным нарушением порядка осуществления своих функциональных обязанностей, которые были установлены законом иным правовым актом, в том числе договором" [56, с. 100-101; 142, с. 71].

Бывают ситуации, когда суды толкуют использование служебного положения не только как совершение действий, находящихся в пределах служебной компетенции виновного лица. Приведем в качестве примера приговор Железнодорожного районного суда г. Пензы от 14 апреля 2011 г. по делу № 1-128/11 в отношении гражданки Ю., работавшей специалистом информационного сервиса ООО "Консультант Пенза". При вынесении приговора суд установил: "Ю. 17 ноября 2010 г. в период времени с 10 до 12 часов, будучи специалистом ООО "КонсультантПенза", осуществляла пополнение правовой системы "КонсультантПлюс" в силу выполнения своих служебных обязанностей в кабинете № 202 старшего следователя СЧ СУ при УВД по Пензенской области Г. Убедившись, что следователь Г. не наблюдает за ее преступными действиями, Ю. в нарушение положений ч. 2 ст. 23 Конституции РФ и Указа Президента РФ от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера", используя свое служебное положение и имея доступ к служебному компьютеру следователя, осуществила неправомерный доступ к охраняемой законом компьютерной информации указанного следователя, без ее согласия скопировала с рабочего стола персонального компьютера на флеш-накопитель папки с файлами документов по уголовному делу №... находившемуся в производстве следователя Г." [148].

Как следует из приведенного в качестве примера приговора Железнодорожного районного суда г. Пензы от 14 апреля 2011 г. по делу № 1-128/11, гражданка Ю., являясь работником сторонней организации и имея доступ к компьютерной технике обслуживаемой организации, признана судом виновной в совершении преступления, предусмотренного ч. 2 ст. 272 УК РФ. Следует отметить, что Ю. не являлась следователем СЧ СУ при УВД по

Пензенской области и в круг ее полномочий не входило ознакомление со служебными делами, находившимися в проидводстве следователя.

Автор разделяет точку зрения, согласно которой под использованием служебного положения понимается использование служащими полномочий, предоставленных им в связи с занимаемой должностью, а также использование авторитета власти или занимаемого служебного положения . В данном случае это лица, которые в силу занимаемой должности или выполняемой работы имеют доступ к компьютеру или их сети (специальный субъект преступления). Это могут быть пользователи компьютеров (программисты, сотрудники IT-отделов и т.п.) либо специалисты, выполняющие абонентское обслуживание компьютеров (приходящие системные администраторы). Эти категории лиц обладают правом санкционированного доступа к компьютерной технике, но, как правило, не имеют доступа к конкретной информации, в отношении которой установлен определенный режим использования. Другими словами, лицо либо самостоятельно осуществляет незаконный доступ к информации (например, подобрав пароль), либо запускает соответствующую программу, цель которой - несанкционированный доступ к информации.

Рассмотрим ситуации, которые возникают в правоприменительной практике и являются предметом исследования ученых-правоведов:

- совершение неправомерного доступа к компьютерной информации лицом, ранее имевшим доступ к компьютерной информации в силу выполняемых им профессиональных обязанностей, но совершившим преступное деяние после окончания права доступа к компьютерной информации. По мнению В.М. Старичкова, привлечение к уголовной ответственности по ч. 2 ст. 272 УК РФ по признаку использования служебного положения зависит от времени возникновения умысла у виновного лица. Если умысел возник во время действия трудовых или гражданско-правовых отношений, то должны вменяться соответствующие квалифицирующие признаки; если же предварительной подготовки не было, а умысел возник уже после того, как лицо утратило право доступа, то нет и квалифицирующих

признаков. На наш взгляд, законодатель связывает совершение преступного деяния и уголовную ответственность по ч. 2 ст. 272 УК РФ именно с правом доступа к компьютерной информации благодаря служебному положению и поэтому совершение неправомерного доступа к компьютерной информации после прекращения выполнения служебных обязанностей не может быть квалифицировано по ч. 2 ст. 272 УК РФ. Ответственность за совершение преступления при таких условиях должна наступать по ч. 1 ст. 272 УК РФ;

- подлежит ли уголовной ответственности по ч. 2 ст. 272 УК РФ лицо, совершившее неправомерный доступ к охраняемой законом компьютерной информации без использования преимуществ занимаемого им служебного положения? Автору близка позиция В.М. Старичкова, который полагает, что в ситуации, когда служебное положение не давало лицу никаких реальных преимуществ при совершении преступного деяния, вменяться данный квалифицирующий признак не должен. Само по себе использование служебного оборудования, программного обеспечения, сетевых реквизитов и т.п. не следует рассматривать как основание повышенной уголовной ответственности. Например, если лицо осуществило неправомерный доступ и скопировало информацию со служебного компьютера, к которому легально имел доступ любой желающий, то ответственность за такое преступление должна наступать по ч. 1 ст. 272 УК РФ [122, с. 92].

За последние несколько лет наблюдается заметное уменьшение количества преступлений данного вида, совершаемых собственными сотрудниками пострадавших организаций. Это может объясняться тем, что большинство уголовных дел по неправомерному доступу возбуждается по самой простой категории дел - дел, связанных с неправомерным доступом к сведениям о логинах и паролях законных пользователей сети Интернет. В настоящее время неправомерный доступ к компьютерной информации собственных сотрудников организация предпочитает не афишировать и соответственно не обращаться в правоохранительные органы, а разобраться с виновным собственными силами [59, с. 30].

В правовой науке одной из дискуссионных тем анализа состава преступления, предусмотренного ст. 272 УК РФ, является характеристика субъективной стороны. Существует точка зрения, в соответствии с которой неправомерный доступ к компьютерной информации может быть совершен только с прямым умыслом [67, с. 665].

Однако, во многих научных работах говорится о возможности совершения неправомерного доступа к охраняемой законом компьютерной информации не только с умыслом, но и по неосторожности. Так, одни авторы указывают, что данное преступление может совершаться как умышленно, так и по неосторожности [68, с. 640]. Такого же мнения придерживается С.Н. Золотухин полагая, что "неосторожная форма вины может проявляться при оценке лицом правомерности своего доступа к компьютерной информации (своеобразная "юридическая ошибка"), а также в отношении неблагоприятных последствий" [58, с. 72].

Следует согласиться с мнением А.Г. Волеводза, который считает, что "субъективная сторона данного преступления характеризуется виной в форме прямого умысла. Косвенный умысел и неосторожная форма вины могут иметь место по отношению к наступлению вредных последствий неправомерного доступа" [36, с. 71].

Указание на то, что неправомерный доступ к компьютерной информации совершается умышленно, содержится и в некоторых источниках информационного права. Так, например, согласно ст. 3 Соглашения о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации, подписанного в г. Минске 1 июня 2001 г., "стороны признают в соответствии с национальным законодательством в качестве уголовно наказуемых следующие деяния, если они совершены умышленно: осуществление неправомерного доступа к компьютерной информации...".

Проанализировав судебную практику по делам о привлечении к ответственности по ст. 272 УК РФ, автор сделал следующий вывод: суды при

разбирательстве уголовных дел устанавливают, что виновные имеют умысел на совершение неправомерного доступа к охраняемой законом компьютерной информации и на достижение последствий в виде уничтожения, копирования, блокирования и модификации компьютерной информации. Например, согласно обвинительному приговору от 13 февраля 2013 г. по делу № 1-12/2013 "мировой суд судебного участка № 45 Егорьевского района Московской области установил преступный умысел, направленный на осуществление неправомерного доступа к охраняемой законом компьютерной информации и ее копирование...". Согласно Постановлению о прекращении уголовного дела за примирением сторон от 14 марта 2012 г. по делу № 1-155/12 Первомайского районного суда г. Ижевска Удмуртской Республики "Х. реализовал свой преступный умысел, осознавая общественную опасность своих действий, предвидя неизбежность наступления общественно опасных последствий, в виде блокирования и модификации компьютерной информации...".

Мотивы и цели неправомерного доступа к компьютерной информации не являются обязательным признаком состава преступления. Однако установление мотива и цели позволяет выявить причины преступления, индивидуализировать ответственность, назначить справедливое наказание. Мотивом преступления признается намерение лица совершить преступления, а целью - результат, к которому это лицо стремится. Корысть, зависть, хулиганство, желание испортить репутацию, месть - основные побуждения к совершению преступления. В некоторых случаях установление мотивов и целей могут существенно повлиять на квалификацию преступления. Так, неправомерный доступ к информации, являющейся государственной тайной, и ее копирование в зависимости от преследуемых преступником целей могут быть квалифицированы как неоконченная государственная измена по ст. 30, 275 УК РФ, если целью была выдача государственной тайны иностранному государству, или по ст. 272 УК РФ, если такой цели не было [75, с. 112].

В.Г. Степанов-Егиянц предлагает включить в качестве квалифицирующего признака в ч. 2 ст. 272 цель скрыть другое преступление

или облегчить его совершение, изложив указанную часть в следующей редакции: "То же деяние, причинившее крупный ущерб, совершенное из корыстной заинтересованности, а равно с целью скрыть другое преступление или облегчить его совершение".

Помимо всего сказанного необходимо отдельно остановится на квалифицированных составах рассматриваемого преступления. Квалифицированный вид неправомерного доступа к компьютерной информации (ч. 2 ст. 272 УК РФ) представляет собой деяние, предусмотренное ч. 1 данной статьи, причинившее крупный ущерб или совершенное из корыстной заинтересованности. Крупный ущерб определен в примечании к ст. 272 УК РФ и применяется для всех составов преступлений гл. 28 УК. Крупным ущербом признается ущерб, сумма которого превышает 1 млн. руб.

Обязательными признаками объективной стороны преступления, предусмотренного ч. 2 ст. 272 УК РФ, являются следующие общественно опасные последствия: - уничтожение, модификация, блокирование или копирование охраняемой законом компьютерной информации; - причиняемый в результате неблагоприятных последствий неправомерного доступа к охраняемой законом компьютерной информации ущерб, сумма которого превышает 1 млн. руб.

Состав преступления, предусмотренного ч. 2 ст. 272 УК РФ, считается оконченным с момента причинения крупного ущерба.. При отсутствии общественно опасного последствия от неправомерного доступа к охраняемой законом компьютерной информации в виде крупного ущерба преступное деяние следует квалифицировать по ч. 1 ст. 272 УК РФ.

Часть 3 ст. 272 УК РФ описывает ответственность за деяния, предусмотренные ч. 1 и 2 данной статьи, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения. Ю.В. Гаврилин отмечает, что совершение неправомерного доступа к компьютерной информации группой лиц, т.е. без предварительного сговора, возможно, но встречается крайне редко

[38, с. 86]. Законодатель, вероятно, посчитал такого рода соисполнительство не достигающим степени общественной опасности, характерной для квалифицированного состава [29, с. 88].

Компьютерные преступления чаще совершаются организованной группой со свойственной ей иерархией и распределением ролей и обязанностей [83, с. 65]. Определения понятий "группа лиц по предварительному сговору" и "организованная группа" даются в ст. 35 УК РФ. Большинство компьютерных преступлений совершаются группой лиц по предварительному сговору, а зачастую организованными группами или преступными сообществами. Более того, уже стали появляться "хакеры-мафиози", единственной целью которых является получение прибыли (мотивом атаки обычного хакера могут быть и хулиганские побуждения).

В случае если одно или несколько лиц на момент совершения неправомерного доступа к компьютерной информации не обладают признаками общего субъекта преступления, предусмотренного ст. 272 УК РФ, преступление нельзя квалифицировать как совершенное группой лиц. Участники неправомерного доступа к компьютерной информации, совершенного группой лиц, должны обладать признаками общего субъекта преступления (возраст, вменяемость).

Неправомерным доступом к компьютерной информации, совершенным группой по предварительному сговору, признается преступление, если в нем участвовали лица, заранее договорившиеся о совместном совершении преступления. Необходимым критерием совершения неправомерного доступа группой по предварительному сговору является "соглашение о совместном участии в преступном посягательстве, которое достигается до момента покушения на него" [139, с. 113].

К субъективным признакам совершения неправомерного доступа к компьютерной информации группой лиц по предварительному сговору относится наличие единого умысла. Для квалификации преступления по ч. 3 ст. 272 УК РФ суды устанавливают возникновение соглашения о совместном

участии до осуществления неправомерного доступа к охраняемой законом компьютерной информации.

В Кассационном определении от 26 апреля 2012 г. по делу № 22-475/2012 судебная коллегия по уголовным делам суда Ямало-Ненецкого автономного округа, рассмотрев в открытом судебном заседании уголовное дело по кассационному представлению государственного обвинителя и кассационной жалобе осужденного Ю. на приговор Новоуренгойского городского суда Ямало-Ненецкого автономного округа от 23 января 2012 г. [145], установила следующее: "По приговору суда Ю., М., С. признаны виновными и осуждены за: - причинение имущественного ущерба ОАО "У" путем обмана при отсутствии признаков хищения, совершенное группой лиц по предварительному сговору, причинившее особо крупный ущерб; - Ю. и М. за неправомерный доступ к охраняемой законом компьютерной информации, совершенный группой лиц по предварительному сговору; С. за те же действия с использованием своего служебного положения".

В качестве доказательства совершения неправомерного доступа к охраняемой законом компьютерной информации группой лиц по предварительному сговору суд обоснованно принял "многочисленную переписку виновных лиц между собой, осуществляемую посредством сети Интернет и обнаруженную на технических устройствах Ю., С., М., в ходе которой осужденные обсуждали факт выявления их преступной деятельности, возможную уголовную ответственность, а также тактику поведения, которой следует придерживаться с целью избежания такой ответственности" [145].

В качестве примера осуществления неправомерного доступа к охраняемой законом компьютерной информации, совершенного организованной преступной группой, приведем уголовное дело в отношении одного из участников организованной преступной группы. 10 марта 2011 г. следователем ГСУ ГУ МВД России по г. Москве возбуждено уголовное дело по ч. 2 ст. 272 УК РФ (неправомерный доступ к компьютерной информации).

В 2010 г. организатор преступной группы, находящийся в федеральном

розыске за побег из исправительной колонии в Смоленской области, приобрел за 550 тыс. долларов в одной из компаний в г. Дубае (ОАЭ) и незаконно ввез в Россию комплекс технических средств, который позволял негласно контролировать каналы связи.

Под его руководством четыре участника организованной преступной группы установили данный комплекс в автомобиль ГАЗ, замаскированный надписями о ремонтных работах. Затем с помощью этого устройства члены ОПГ осуществляли неправомерный доступ к компьютерной информации операторов сотовой связи, затем копировали данные с мобильных телефонов проходящих мимо машин граждан и путем инициирования исходящих вызовов и СМС-сообщений определенным образом модифицировали в системах ЭВМ информацию. Таким образом, злоумышленники незаконно завладевали денежными средствами граждан в различных районах Москвы, а также Брянской, Московской, Орловской и Смоленской областях [163].

Как следует из приведенного примера, у организованной преступной группы был руководитель, распределявший роли между соучастниками, всех соучастников объединял единый умысел, направленный на совершение преступления, предусмотренного ст. 272 УК РФ.

Автор согласен с мнением ученых, считающих недостатком законодательства совмещение в ст. 272 УК РФ квалифицирующих признаков "совершение преступления группой лиц по предварительному сговору или организованной группой". По мнению ученых, неразумно совмещать в одном пункте статьи разные по силе влияния обстоятельства, используемые в других главах УК РФ для конструирования квалифицированных и особо квалифицированных видов преступления [43, с. 62].

Квалифицированный вид неправомерного доступа к компьютерной информации (ч. 4 ст. 272 УК РФ) представляет собой деяния, предусмотренные ч. 1 - 3 данной статьи, если они повлекли тяжкие последствия или создали угрозу их наступления. В диспозиции ст. 272 УК РФ понятие "тяжкие последствия" не раскрывается, оно является оценочным и должно определяться

судом в каждом конкретном случае в зависимости от обстоятельств дела.

К тяжким последствиям неправомерного доступа к компьютерной информации могут быть отнесены внедрение в системы, регулирующие безопасность жизни и здоровья граждан (например, в диспетчерские системы на транспорте, особенно воздушном, системы, обеспечивающие обороноспособность страны, отвечающие за экологическую безопасность), случаи гибели людей либо причинения тяжкого вреда здоровью, а также значительного экономического ущерба государству, юридическим и физическим лицам в результате дезорганизации работы производственных комплексов, нарушения организованной работы транспорта, уничтожения или повреждения имущества. Указание на то, какие последствия могут рассматриваться в качестве тяжких, уместно дать в отдельном постановлении Пленума Верховного Суда РФ.

При этом возможна квалификация по совокупности с иными тяжкими преступлениями, предусматривающими аналогичные последствия по неосторожности. Так, неправомерный доступ к охраняемой законом компьютерной информации (например, в силу нарушения технологического процесса на производстве), в результате которого по неосторожности наступила смерть человека, должен квалифицироваться по совокупности [131, с. 281].

# ГЛАВА 2. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ ПРОГРАММ

## 2.1. ОБЪЕКТИВНЫЕ ПРИЗНАКИ СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Статья 273 УК РФ предусматривает ответственность за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования информации или нейтрализации средств защиты компьютерной информации. Одним из наиболее опасных деяний из всего спектра компьютерных преступлений считается использование и распространение вредоносных программ, причиняющих вред компьютерной информации, системам ее обработки и передачи [89, с. 12]. По мнению самого законодателя, это преступление является самым общественно опасным деянием из всех компьютерных преступлений. О такой позиции законодателя свидетельствуют размер санкций (до семи лет лишения свободы по ч. 3 ст. 273) и конструирование ст. 273 по типу формальных составов. ФЗ "О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ" законодатель повысил уголовную ответственность за создание, использование и распространение вредоносных программ.

Статистика уголовных дел, возбуждаемых по статьям гл. 28 УК РФ, свидетельствует о том, что в большинстве случаев применяется ст. 273 УК РФ. Так, в 2017 г. судами было возбуждено 64 дела по ст. 272 УК РФ и лишь 91 дело по 273 УК РФ. Что касается ст. 274, то в 2017 г. судами не было рассмотрено дел. За первое полугодие 2018 г. по ст. 272 УК РФ судами возбуждены 29 дел, по ст. 273 УК РФ - 79 дел и по ст. 274 УК РФ - 0.

В результате совершения преступления, предусмотренного ст. 273 УК РФ, нарушается нормальное функционирование компьютерной системы.

Следствием запуска вредоносной программы является нарушение нормального порядка работы компьютерных программ, что может выражаться в невыполнении команд пользователя, невозможности запуска программ, открытия тех или иных файлов.

Понятия родового и видового объектов преступлений в информационной сфере были рассмотрены нами ранее. В данной главе будет исследован непосредственный объект преступления, предусмотренного ст. 273 УК РФ. Непосредственным объектом преступлений в сфере компьютерной информации являются конкретные общественные отношения, указанные в диспозициях соответствующих статей [84, с. 9]. Для оценки характера и степени общественной опасности деяния и его правильной квалификации важно уяснить особенности непосредственного объекта преступлений в сфере компьютерной информации [83, с. 196].

А.Г. Волеводз под непосредственным объектом данного преступления понимает правоотношения в сфере обеспечения безопасного производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и потребления компьютерной информации, использования информационных компьютерных технологий и средств их обеспечения, защиты компьютерной информации и прав субъектов, участвующих в информационных процессах и информатизации с использованием компьютеров, их систем и сетей [36, с. 72].

Под непосредственным объектом исследуемого преступления автор полагает правильным понимать общественные отношения, обеспечивающие право обладателя компьютерной информации на ее безопасное создание, хранение, использование и передачу.

Наибольший интерес у ученых вызывает содержание предмета преступления, предусмотренного ст. 273 УК РФ. Соотношение объекта и предмета преступного посягательства в сфере компьютерной информации особенно важно ввиду того, что компьютер и компьютерная информация в таких особых формах представляют собой особую материю [83, с. 199].

Некоторые ученые придерживаются мнения, что предметом исследуемого

преступления является компьютерная информация [44, с. 124]. Другие исследователи считают предметом преступления, предусмотренного ст. 273 УК РФ, программы: программы для ЭВМ и машинный носитель с такой программой; вредоносные программы; вредоносные программы или их носители. Т.М. Лопатина, Е.А. Маслакова рассматривают вредоносную программу как "разновидность компьютерной информации, содержащей определенные сведения, компилированные в читаемый набор машинных символов" [83, с. 207; 91, с. 79].

Рассмотрим, что представляют собой вредоносные компьютерные программы. Следует сразу отметить, что, к сожалению, в уголовном законодательстве понятие "вредоносная программа" отсутствует. Статья 273 УК РФ лишь указывает на негативные последствия, связанные с действием таких программ. Отсутствие такого определения, на наш взгляд, является пробелом в законодательстве РФ. А.В. Суслопаров также считает, что при отсутствии четкого ответа на вопрос о том, какую программу признавать вредоносной, "невозможно эффективное применение рассматриваемой нормы на практике" [127, с. 139].

В отсутствие нормативного определения понятия вредоносной программы наука выработала ряд подходов к решению данного вопроса. Так, Т.Г. Смирнова считает, что вредоносная программа - это компьютерная программа, способная к саморазмножению, либо входящая в структуру безопасной программы, имеющая целью уничтожение информации, либо аккумулирующая ее определенные категории, либо присваивающая программе не свойственные ей функции, что заведомо нарушает нормальное функционирование ЭВМ [118, с. 18]. М.Ю. Дворецкий полагает, что такое определение перегружено терминами, отсутствующими в уголовно-правовой науке. Ученый предлагает собственное определение понятия "вредоносная программа" через цели, для достижения которых она создается. Под вредоносной он понимает программу, специально разработанную или модифицированную для несанкционированных уничтожения, блокирования,

модификации либо контролирования информации [51, с. 112].

Интересна позиция некоторых авторов, определяющих вредоносность программы не ее назначением и способностью уничтожать, блокировать, модифицировать, копировать информацию, а тем, предполагает ли ее действие, во-первых, предварительное уведомление собственника компьютерной информации или другого добросовестного пользователя о характере действия программы, а во-вторых, получение его согласия (санкции) на реализацию программой своего назначения. Нарушение одного из требований делает программу для ЭВМ вредоносной [27, с. 114; 36, с. 74; 44, с. 126; 91, с. 69].

В связи с тем, что вредоносная компьютерная программа является разновидностью компьютерной программы, необходимо более подробно рассмотреть толкование понятия "программа для ЭВМ". Его определение дано в ст. 1261 ГК РФ [2]. В ней под понятием "программа для ЭВМ" понимается представленная в объективной форме совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств, таким образом, чтобы достигался определенный результат, включая подготовительные материалы, полученные в ходе разработки программы для ЭВМ, и порождаемые ею аудиовизуальные отображения. Действующий ГК РФ использует весьма устаревшее понятие "ЭВМ", в то время как УК РФ оперирует понятием "компьютерная программа".

Определение вредоносной программы дается в п. 2.6.5 ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", утвержденного Приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст. Вредоносной является программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы. В свою очередь, несанкционированное воздействие на информацию представляет собой воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате,

уничтожению или сбою функционирования носителя информации.

Кроме того, определение понятия "вредоносная программа" содержится в Соглашении о сотрудничестве государств - участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (г. Минск, 1 июня 2001 г.). Согласно п. "в" ст. 1 вышеназванного документа "вредоносная программа - созданная или существующая программа со специально внесенными изменениями, заведомо приводящая к несанкционированным уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети". По мнению А.В. Геллера, такое определение вредоносной программы является "наиболее приемлемым" [44, с. 141].

В Постановлении Правительства РФ от 10 сентября 2007 г. № 575 "Об утверждении Правил оказания телематических услуг связи" [17] дается определение вредоносного программного обеспечения, под которым понимается программное обеспечение, целенаправленно приводящее к нарушению законных прав абонента и (или) пользователя, в том числе к сбору, обработке или передаче с абонентского терминала информации без согласия абонента и (или) пользователя либо к ухудшению параметров функционирования абонентского терминала или сети связи. Результатом запуска вредоносной программы является нарушение нормального порядка работы программ, что может выражаться в невыполнении команд пользователя, невозможности запуска программ, открытия тех или иных файлов.

По мнению автора из приведенных выше нормативных определений вредоносной компьютерной программы наиболее полным и удачным является определение, содержащиеся в ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения".

Анализ приведенных выше нормативно-правовых актов свидетельствует о том, что законодатель при определении вредоносной компьютерной программы не применяет единые технические термины. Например, в соответствии с диспозицией ст. 273 УК РФ вредными последствиями

воздействия вредоносных программ на компьютерную информацию являются уничтожение, блокирование, модификация, копирование компьютерной информации и нейтрализация средств защиты, а согласно нормам, изложенным в вышеназванном ГОСТе, негативными последствиями признаются утечка, искажение, подделка, уничтожение, блокирование доступа к информации, а также утрата, уничтожение или сбой функционирования носителя информации. При этом содержание ни одного из данных понятий нормативно не определено, что создает неопределенность в правоприменении.

Как видно, общими для текстов УК РФ и ГОСТа являются такие понятия, как "уничтожение" и "блокирование". При анализе вышеназванных актов возникает следующий вопрос: например, каково соотношение понятий "модификация компьютерной информации" (УК РФ) и "искажение компьютерной информации" (ГОСТ)? Модификацией компьютерной информации является любое изменение первоначального состояния информации, не меняющее сущность объекта. Например, изменение названия текстового файла с "книга.doc" на "лучшая_книга.doc".

Утечка информации представляет собой неконтролируемое распространение информации за пределы защищаемой зоны ее функционирования, если в результате этого произошло получение информации (ознакомление с ней) лицами, не имеющими к ней права доступа. Утечка информации может происходить по различным информационным каналам, при обмене пользователями средствами хранения компьютерной информации.

ГОСТ относит к вредным последствиям действия вредоносных программ физическую порчу носителей информации, что существенно расширяет и уточняет перечень негативных последствий в ГОСТе по сравнению с УК РФ. Думается, что наличие данного последствия в ст. 272 и 273 УК РФ положительно бы влияло на правоприменительную практику.

В целях единства применения и толкования законодательства возможно дополнить ст. 273 УК РФ примечанием следующего содержания: "Под вредоносной компьютерной программой понимается представленная в

объективной форме совокупность данных и команд, предназначенных для воздействия на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящая к уничтожению, модификации, копированию, блокированию, искажению, утечке, подделке, а также к утрате, уничтожению или сбою функционирования носителя информации". В данном определении нашли бы отражение все возможные последствия, упоминаемые в действующих нормативных актах РФ.

Рассмотрим основные виды вредоносных компьютерных программ. В зависимости от механизма действия к ним относятся: - "логическая бомба"; - "червь"; - "троянский конь";- компьютерный вирус.

"Логическая бомба" - программа, которая запускается при определенных временных или информационных условиях для осуществления вредоносных действий (как правило, несанкционированного доступа к информации, искажения или уничтожения данных). Примерами таких условий могут быть: наступление заданной даты, переход в определенный режим работы, наступление некоторых событий заданное число раз и т.п.

"Червь" ("сетевой червь") - это вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, необязательно совпадающих с оригиналом. Лавинообразное размножение программ приводит к перегрузке каналов связи, памяти и к блокировке системы.

"Троянский конь" - это вредоносный код, совершающий не санкционированные пользователем действия (например, кража информации, уничтожение или модификация информации, использование ресурсов машины в злонамеренных целях и т.п.). "Троянский конь" является наиболее распространенным в киберсреде, так как существует множество конструкторов, позволяющих даже неопытному пользователю создавать собственные программы данного типа.

Компьютерный вирус - это программа, способная создавать свои

дубликаты (необязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и (или) файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

К вредоносным программам вплотную примыкает опасная дезинформация. Иногда то, что не может сделать вредоносная программа, удается сделать руками самих пользователей. Можно привести следующий пример. Пользователь получает электронное письмо, содержащее примерно такой текст: "Внимание! Антивирусная тревога! По сети распространяется новый, очень опасный вирус. Проникая в компьютер, он принимает вид обычного системного файла и какое-то время ничем себя не проявляет. Затем в случайно определенное время он уничтожает все пользовательские файлы и стирает BIOS. Если мы успели Вас вовремя предупредить, Вы еще успеете его обезвредить. Откройте папку "Wi№dows/System32", найдите в ней файл с изображением... и немедленно удалите его". Остальное выполняется руками пользователя, и в таком случае сложно говорить о возможностях привлечения злоумышленника к уголовной ответственности, по крайней мере с учетом современной правоприменительной практики.

Отметим, что ряд ученых отождествляют понятие "вредоносная программа" с категорией "компьютерный вирус" [133, с. 559]. Ошибочно ставить знак равенства между вирусной и вредоносной программой, как это делают некоторые специалисты [131, с. 605]. Смешение понятий "вредоносная" и "вирусная" ведет к неоправданному сужению признаков объективной стороны рассматриваемого преступления, что создает возможность для безнаказанности за создание, использование и распространение вредоносных программ для ЭВМ, не являющихся по своим качественным характеристикам вирусными [108, с. 39]. Мы согласны с этой точкой зрения и считаем, что компьютерный вирус есть лишь разновидность вредоносных компьютерных программ.

С нашей точки зрения, компьютерной информации, безусловно,

причиняется вред вредоносными программами, поэтому она является предметом исследуемого деяния. Следует подчеркнуть, что если в ст. 272 УК РФ предметом преступного посягательства считается "охраняемая законом компьютерная информация", то согласно ст. 273 УК РФ уголовно-правовой защите подлежит "компьютерная информация". В данном случае такой защите подлежит любая информация независимо от того, имеет ли она собственника (законного владельца) или предназначена для широкого круга лиц [83, с. 205].

Суды рассматривают в качестве предмета преступления, предусмотренного ст. 273 УК РФ, именно компьютерную информацию. Например, из Постановления Первомайского районного суда г. Ижевска от 22 марта 2012 г. о прекращении уголовного дела № 1-162/12 [162] в отношении гражданина В. следует, что подсудимый В. совершил распространение компьютерных программ, заведомо предназначенных для несанкционированной модификации компьютерной информации. Мы видим, что вред преступными действиями подсудимого нанесен компьютерной информации.

Согласно ч. 1 ст. 273 УК РФ объективной стороной исследуемого преступления являются следующие альтернативные действия: создание, распространение или использование компьютерных программ или иной компьютерной информации, заведомо предназначенных для уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты таковой. Объективная сторона преступления, предусмотренного ст. 273 УК РФ, может заключаться только в совершении активных действий [83, с. 213; 44, с. 124]. А.А. Каспаров определяет объективную сторону преступления, предусмотренного данной статьей, как общественно опасное деяние, посредством компьютерного вируса нарушающее безопасность и нормальный порядок законного использования компьютерной информации [62, с. 24].

Создание, использование и распространение вредоносных компьютерных программ считаются оконченными с момента создания такой программы,

внесения изменений в существующие программы, использования либо распространения подобной программы вне зависимости от наступления вредных последствий. Само совершение перечисленных действий уже столь опасно, что излишне дожидаться наступления вреда от них [84, с. 9; 61, с. 101].

В уголовно-правовой доктрине существует и другая точка зрения, согласно которой "до сих пор не было приведено каких-либо "весомых" аргументов в пользу того, что деяния, предусмотренные ст. 273 УК РФ, представляют какую-то чрезвычайную угрозу или особую опасность, требующую исключительного подхода при криминализации" [141, с. 67]. С точки зрения сторонников такого взгляда, в диспозиции ст. 273 УК РФ "самый главный недостаток - формальный состав" [141, с. 71].

Противником формального состава преступления, предусматривающего ответственность за создание, использование, распространение вредоносных программ, выступает С.Д. Бражник. По его словам, "в мире пока не зафиксировано ни одного случая наступления тяжких последствий из-за внедрения вредоносной программы". Кроме того, ученый считает, что хакеров высокого класса мало, а большая часть действий связана с непрофессионалами, использующими стандартные средства и методы проникновения в компьютерные системы. Отрицательным результатом формальности состава деяния, предусмотренного ст. 273 УК РФ, ученый называет подпадание под уголовно-правовую репрессию деяний, "которые во многих случаях по степени вредоносности не выходят за рамки административного правонарушения, т.е. недотягивают до уровня общественной опасности, характерной для преступлений".

Сторонником введения административной ответственности за создание, распространение или использование вредоносных программ, не причинивших значительного ущерба обладателю информации, выступила Л.А. Букалерова. По мнению ученой, такие деяния "не являются общественно опасными и должны быть декриминализированы". С.Ю. Бытко считает, что "вполне допустимо применение мер административного воздействия". С.А. Кодинцев

дальнейшее совершенствование действующей редакции ст. 273 УК РФ видит в переносе наименее опасных деяний, определенных в диспозиции данной статьи, из разряда уголовно наказуемых в категорию административных правонарушений.

Автор считает возможным поддержать действующую формулировку закона и разделяет позицию М.М. Малыковцева, считающего вполне целесообразным решение, принятое в свое время законодателем, о том, что конструкция состава, предусматривающего ответственность за создание, использование и распространение вредоносных программ, должна быть формальной.

Созданные преступником программы должны содержать в себе потенциальную угрозу уничтожения, блокирования, модификации либо копирования компьютерной информации или нейтрализации ее средств защиты. Совершение любого из перечисленных ниже действий является достаточным для признания деяния оконченным, даже если программа реально не причинила вреда информационным ресурсам или компьютеру: 1) создание программы для компьютера (программирование) или иной компьютерной информации, т.е. проектирование программы, построение алгоритмов, разработка структур данных, написание текста программы; 2) отладка и тестирование программы (испытание программы); 3) документирование, настройка (конфигурирование), доработка и сопровождение вредоносной компьютерной программы.

В зависимости от способа возникновения вредоносных программ создание компьютерных программ можно разделить на две группы: создание вредоносных программ и внесение изменений в уже существующие программы.

Уголовная ответственность наступает по ст. 273 УК РФ независимо от того, использовалась программа или нет. Использование вредоносной программы или иной компьютерной информации означает совершение любых действий по введению ее в оборот с целью достижения преступного результата. Ряд ученых определяют использование вредоносных программ как "выпуск в

свет, воспроизведение и иные действия по введению их в оборот" [72, с. 695] (например, посредством размещения в компьютерной сети, установки на жесткий диск пользователя в процессе технического обслуживания компьютера) [20, с. 572] или путем записи программы в память ЭВМ на материальный носитель, распространения по сетям либо путем иной передачи другим лицам [117, с. 31-32].

В.В. Воробьев отмечает, что "термин "воспроизведение" наиболее точно выражает суть такого действия" [37, с. 94]. Думается, что такое понимание содержания понятия "использование" близко к содержанию понятия "распространение".

А.А. Каспаров и М.М. Малыковцев начало использования вредоносной программы ставят в зависимость от свойств самой программы: "Если она рассчитана на немедленные вредоносные действия, использование наступает с момента ее исполнения на ЭВМ, если же в вирусе заложены свойства "бомбы" - с момента проявления этих свойств". Аналогичную позицию разделяет Ю.А. Красиков, понимающий под использованием вредоносных программ "обращение, употребление их по назначению, приведение в действие, когда они начинают проявлять вредные качества".

В правовой науке ведется дискуссия о том, любое ли создание, распространение или использование компьютерных программ, заведомо приводящее к несанкционированным копированию, модификации, блокированию или уничтожению компьютерной информации, является уголовно наказуемым преступлением. Например, В.Ю. Максимов утверждает, что "вирусы подразделяются на безвредные, неопасные, опасные и очень опасные" [87, с. 91]. По мнению В.В. Крылова, "инфекции проникновения" вообще не уничтожают информацию, не блокируют доступ к ней" [79, с. 101].

На наш взгляд, не будет являться уголовно наказуемым создание, использование вредоносных программ организациями, осуществляющими разработку антивирусных программ (Антивирус Касперского, DrWeb, Avast и проч.), поскольку такая деятельность имеет целью совершенствование

программно-технических средств защиты компьютерной информации.

Таким образом, создание специальных программ, обладающих в том числе и вредоносными свойствами (в их уголовно-правовом понимании), может считаться одним из средств защиты информации, средством контроля эффективности защиты информации, а также одним из способов проведения специальных мероприятий при осуществлении контртеррористической операции.

Близкой по содержанию позиции придерживается В.Ю. Максимов, утверждающий, что "нельзя запрещать любое создание компьютерных вирусов, обладающих вредоносными свойствами, т.к. это может происходить и в общественно полезных целях" [87, с. 92]. У.В. Зинина обращает внимание на то, что "в ряде случаев использование подобных программ не будет являться уголовно наказуемым, поскольку это относится к деятельности организаций, осуществляющих разработку антивирусных программ".

Легальное определение понятия "распространение информации" содержится в п. 9 ст. 2 ФЗ "Об информации, информационных технологиях и о защите информации" [13], согласно которому распространением информации признаются действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц.

Суды оценивают продажу как один из способов распространения вредоносных компьютерных программ. В приговоре от 11 октября 2011 г. по делу № 1-301/2011 [147] Вязниковский городской суд Владимирской области признал виновным гражданина РФ (Ф.И.О. обезличены) в совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ. Суд установил, что Ф.И.О., действуя умышленно, осознавая, что он распространяет путем продажи программы для ЭВМ, заведомо приводящие к несанкционированной модификации либо копированию информации, путем продажи контрафактных экземпляров программного обеспечения в помещении магазина с целью последующего приведения распространяемых им контрафактных экземпляров

программ в работоспособное состояние, распространил путем продажи программу, основным предназначением которой является преодоление встроенной защиты программы путем ее нейтрализации, а именно достижения работоспособности программы без электронного ключа защиты путем блокирования обращений программы к электронному ключу защиты, входящему в лицензионную поставку и являющемуся его составной неотъемлемой частью [147].

Рассмотрим основные научные идеи и предложения по совершенствованию конструкции диспозиции ч. 1 ст. 273 УК РФ. Ученые предлагают криминализировать не только создание, распространение и использование компьютерных программ и иной компьютерной информации, но и посредническую деятельность по приобретению вирусной программы и ее хранению. Можно признать отсутствие хранения и приобретения вредоносных компьютерных программ в перечне деяний, образующих объективную сторону преступления, предусмотренного ч. 1 ст. 273 УК РФ, определенным пробелом законодательства.

Для привлечения к уголовной ответственности необходимо осознание лицом вредоносности программы, которую он приобретает. Что же касается причин и целей такого приобретения, то нам представляется, что для квалификации деяния как преступления они не должны иметь значения, хотя должны учитываться при индивидуализации наказания. Целесообразно считать приобретение оконченным с момента перехода вирусной программы во владение приобретшего лица.

Под хранением вируса ученые предлагают понимать сам процесс владения, нахождение его у виновного лица, содержание в сохранности, фактическое обладание названной программой. Правы исследователи, считающие, что хранение характеризуется бездействием и является длящимся процессом, завершающимся в тот момент, когда предмет преступления окончательно выйдет из владения виновного лица [91, с. 226].

Суды при вынесении приговора о признании лица виновным в

использовании и распространении вредоносных компьютерных программ устанавливают, что этим действиям, входящим в состав объективной стороны ст. 273 УК РФ, предшествуют, как правило, приобретение и хранение таких программ. При установлении ответственности за хранение и приобретение вирусных программ, возможно, удалось бы избежать дальнейших общественно опасных последствий, наступающих при использовании и распространении таких программ.

При наличии в законодательстве РФ норм уголовной ответственности за хранение и приобретение вредоносных компьютерных программ Т. был бы привлечен к уголовной ответственности до возникновения угрозы уничтожения, модификации, копирования, блокирования компьютерной информации.

Рассмотрим позиции ученых относительно возможных последствий, для достижения которых и предназначены вредоносные компьютерные программы. В литературе высказаны мнения, что существующая редакция недостаточно корректна. Так, С.А. Кодинцев полагает, что последствие в виде "несанкционированного уничтожения" должно быть более конкретизировано, поскольку уничтожение информации в большинстве случаев является восполнимым либо информация не представляет для пользователя конкретной ценности. Ученый предлагает отнести к числу последствий "несанкционированное невосполнимое уничтожение информации", значимой для пользователя [74, с. 15-17].

Такое предложение трудно признать последовательным. Думается, что для квалификации действий преступника не имеет значения, осведомлен ли злодей о ценности информации для пользователя или нет, а также может ли такая информация быть восстановлена или нет. Умысел виновного направлен на заведомое уничтожение компьютерной информации.

Определенные вопросы вызывает такое последствие создания, использования или распространения вредоносных программ, как нейтрализация средств защиты компьютерной информации. Данное последствие было

включено в УК РФ ФЗ "О внесении изменений в Уголовный кодекс РФ и отдельные законодательные акты РФ".

Определение понятия "защита информации" содержится в ГОСТ Р 50922-2006 "Защита информации. Основные термины и определения", согласно п. 2.1.1 названного документа под защитой информации следует понимать деятельность, направленную на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. Защита информации - это совокупность мер, обеспечивающих безопасность прав владельцев информационной продукции, в первую очередь программ, баз и банков данных, от несанкционированного доступа, использования, разрушения или нанесения ущерба в какой-либо иной форме [44, с. 48].

К техническим средствам относятся изделия, оборудование, аппаратура и (или) их составные части, функционирующие на основании законов электротехники, радиотехники и (или) электроники и содержащие электронные схемы и (или) компоненты. К криптографическим средствам защиты можно отнести любые способы секретной записи и механическое либо электрическое устройство, используемые в целях маскировки или сокрытия содержания, значимости или смысла передаваемой информации. ГОСТ Р 50922-2006" Защита информации. Основные термины и определения", утвержденный Приказом Ростехрегулирования от 27 декабря 2006 г. № 373-ст, относит к криптографическим такое средство защиты информации, которое реализует алгоритмы криптографического преобразования информации.

Программные средства - это средства, предусматривающие определенную последовательность процедур, направленных на защиту компьютерной информации. Программные средства в компьютерном смысле - это объективная форма представления совокупности данных и команд, предназначенных для функционирования компьютерных устройств, с целью получения определенного результата, включая подготовительные материалы, полученные в ходе разработки компьютерной программы, и порождаемые ею

аудиовизуальные отображения.

Программные средства защиты содержат механизм мандатного разграничения доступа. Система принимает решение о возможности доступа субъекта к объекту или о запрете доступа, принимая за основание тип операции, связанный с каждым субъектом, и мандатную метку, связанную с объектом. Как правило, средства защиты информации содержатся в ядре операционной системы, но идентификация, аутентификация и контроль целостности файлов являются отдельными программными компонентами.

Помимо очевидного взлома программ антивирусной защиты под нейтрализацию может подпасть и следующая ситуация. Зачастую пользователи выкладывают лицензионное программное обеспечение вместе с программами, с помощью которых можно взломать защиту лицензионного программного обеспечения и использовать его несколько раз. К таким программам относятся: 1) "кейген" (от англ. keygen - keyge№erator - генератор ключей) - это программа, которая генерирует либо криптографические ключи для шифрования данных, либо псевдоподлинные CD-ключи или серийные, регистрационные или активационные номера для регистрации или активирования программного обеспечения; 2) "крэк" (от англ. crack - разламывать, раскалывать) - специальная программа для взлома программного обеспечения. Формально под действие ст. 273 УК РФ может подпасть очень большое количество пользователей сети Интернет, которые используют "взломанное" программное обеспечение.

С.Ю. Бытко считает неоправданным включение законодателем понятия "нейтрализация средств защиты" в состав объективной стороны преступления [34, с. 16-19]. Ученый считает, что действия по нейтрализации средств защиты не должны получать самостоятельной правовой оценки, поскольку применяются лицом, как правило, в качестве подготовительного этапа для неправомерного доступа к информации с целью ее последующего уничтожения , блокирования, модификации или копирования [34, с. 19]. Автор разделяет эту позицию и полагает, что нейтрализация средств защиты не является целью

совершения преступления, предусмотренного ч. 1 ст. 273 УК РФ.

Анализ судебной практики подтверждает, что использование компьютерных программ нейтрализации средств защиты есть средство к получению неправомерного доступа к компьютерной информации.

Следует отметить, что формулировка объективной стороны ст. 273 УК РФ не лишена недостатков. Анализ новой редакции рассматриваемого состава УК РФ позволяет сделать вывод, что, к сожалению, не все проблемы были решены ФЗ "О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации". Т.Л. Тропина справедливо отмечает, что безусловным недостатком законодательной техники как в прежней, так и в действующей редакции ст. 273 УК РФ является "синонимия единственного или множественного числа" [130, с. 207].

На данный недостаток обращает внимание и С.Д. Бражник, поскольку исходя из буквального толкования нормы (ст. 273 УК РФ) следует, что создание одной вредоносной программы; внесение одного изменения в одну из программ; использование или распространение одной вредоносной программы или одного из носителей компьютерной информации, содержащего одну вредоносную программу, уголовно ненаказуемы [29, с. 89]. Такое толкование явно противоречит смыслу рассматриваемой статьи. Автор разделяет мнение С.Д. Бражника, который называет такую ситуацию нонсенсом.

## 2.2. СУБЪЕКТИВНЫЕ ПРИЗНАКИ СОЗДАНИЯ, ИСПОЛЬЗОВАНИЯ И РАСПРОСТРАНЕНИЯ ВРЕДОНОСНЫХ КОМПЬЮТЕРНЫХ ПРОГРАММ

Согласно положениям доктрины создание, использование и распространение вредоносных программ и иной компьютерной информации совершается только с прямым умыслом [57, с. 146]. В силу того что состав преступления, предусмотренного ст. 273 УК РФ, "сформулирован как формальный, вина лица должна всегда быть выражена в виде прямого умысла" [91, с. 96].

Субъективная сторона характеризуется только прямым умыслом, когда виновный осознает общественную опасность своих действий, предвидит возможность наступления общественно опасных последствий и желает их наступления. Если вирусописатель, создавая программу, не предвидит того, что в итоге ее действия могут реально произойти уничтожение, модификация, блокирование либо копирование какой-либо информации, т.е. не осознает характера ее общественной опасности, оно не подлежит уголовной ответственности.

В уголовно-правовой науке имеет место и другая точка зрения, сторонники которой утверждают, что преступление, предусмотренное ч. 1 ст. 273 УК РФ, может быть совершено не только с прямым, но и с косвенным умыслом. Иначе говоря, виновное лицо осознавало общественно опасный характер своих действий по созданию, использованию или распространению программы, которая способна уничтожить, блокировать, модифицировать либо копировать компьютерную информацию, нарушить работу ЭВМ, системы ЭВМ или их сети, желало или сознательно допускало наступление вредоносных последствий или относилось к ним безразлично [132, с. 356].

В отечественной юридической науке есть мнение, что исследуемое преступление может совершаться как по неосторожности в виде легкомыслия, так и с косвенным умыслом в виде безразличного отношения к возможным последствиям, По мнению К.Н. Евдокимова, неосторожность в форме легкомыслия или небрежности может быть по отношению к наступившим последствиям. В связи с этим ученый считает: "Законодатель совершенно напрасно исключил из диспозиции рассматриваемой статьи квалифицирующий признак "те же деяния, повлекшие по неосторожности тяжкие последствия". Автор считает, что действовать при совершении исследуемого состава по неосторожности нельзя. При совершении преступления, предусмотренного ч. 1 ст. 273 УК РФ, с прямым умыслом необходимо установить, что уровень осведомленности совершившего преступление лица о вредоносности компьютерной программы должен быть достаточно высок и лицо должно было

желать наступления вредоносных последствий.

На практике, конечно, не исключены ситуации, когда лицо, совершившее анализируемое преступление, было осведомлено о вредоносных свойствах программы, однако не желало проявления ее вредоносных свойств или заблуждалось относительно вредоносных качеств такой программы, что означает совершение преступления, предусмотренного ст. 273 УК РФ, с косвенным умыслом.

В.В. Воробьев полагает, что признак допущения виновным того, что программа приводит к указанным в диспозиции ст. 273 УК РФ последствиям, заменяет собой такой признак интеллектуального момента прямого умысла, как предвидение возможности наступления общественно опасных последствий в материальном составе преступления. В то время как признак знания тех же обстоятельств в исследуемом нами составе преступления заменяет признак предвидения неизбежности наступления таких последствий [37, с. 129].

Ранее вредоносная программа должна была заведомо приводить к "несанкционированному уничтожению, блокированию, модификации либо копированию информации", т.е. лицо должно было точно знать, что такая программа может выполнять перечисленные функции. В новой редакции ст. 273 УК РФ слова "заведомо приводить" заменены на слова "заведомо предназначенные", означающие, что программа или иная компьютерная информация создавалась, распространялась или использовалась для совершения несанкционированных уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, но при этом для наличия состава преступления не требуется ее фактической способности приводить к перечисленным последствиям, например, из-за ошибки преступника.

Суды придерживаются мнения, что исследуемое преступное деяние совершается с умышленной формой вины. 10 июня 2004 г. Тракторозаводским районным судом г. Челябинска вынесен приговор в отношении А. Судом установлено, что А., обладая достаточными знаниями в области

информационных технологий, навыками обработки информации и пользования компьютерной техникой, опытом работы в глобальной сети Интернет, владея языком программирования, имея умысел на создание и использование программы ЭВМ, заведомо приводящей к несанкционированному блокированию, копированию информации, в феврале 2003 г. в г. Челябинске создал программу для ЭВМ "se№dsms.pl" для массовой рассылки коротких текстовых сообщений (СМС-сообщений) на сайт ЗАО "Л" с адресом в сети Интернет www.megafo№ural.ru и через него на машинные носители абонентов, заведомо приводящую к несанкционированному блокированию, копированию информации, а в дальнейшем использовал данную программу.. 8 февраля 2003 г. А. на своем персональном компьютере, установленном у него дома, желая убедиться в работоспособности созданной им программы "sendsms.pl", в строке задания параметров, необходимых программе рассылки СМС-сообщений, ввел данные, позволяющие сделать рассылку 10 нецензурных текстовых сообщений одинакового содержания абоненту сети "Мегафон" с номером телефона *****, принадлежащим *****, после чего привел программу в действие.. В результате действия указанной программы абонент с номером телефона ***** получил 10 СМС-сообщений, т.е. произошло копирование (рассылка) компьютерной информации с сервера ЗАО "Л" на телефонный аппарат, являющийся машинным носителем ЭВМ. Убедившись в работоспособности компьютерной программы "se№dsms.pl", у А. возник умысел на осуществление массовой рассылки СМС-сообщений нецензурного содержания всем абонентам Челябинского фрагмента сети "Мегафон" ЗАО "У". Исполняя задуманное и достоверно зная, что использование данной программы повлечет за собой несанкционированное блокирование, копирование информации, 23 мая 2003 г. в 00 часов 22 минуты А., находясь у себя дома, пытаясь скрыть следы своей преступной деятельности, воспользовался известными ему от № логином (регистрационное имя пользователя для доступа к сайту) ***** и соответствующим ему паролем *****, которые № использовал для выхода на свой сайт, размещенный на сервере ООО "Y" г. Санкт-Петербурга, и с

помощью своего персонального компьютера и модема зашел на указанный сайт. Там А. разместил программу "se№dsms.pl", в которую заложил текст СМС-сообщения нецензурного содержания. После этого, не уведомляя собственника компьютерной информации о характере выполняемых программой функций и не получив согласия на реализацию программой своего назначения, привел указанную программу, в которой была заложена функция автоматической рассылки СМС-сообщений с использованием услуги по отправке СМС на сайте www.megafonural.ru компании ЗАО "Уральский Джи Эс Эм", в действие [159].

Как следует из приведенных выше выдержек из приговора от 10 июня 2004 г. Тракторозаводского районного суда г. Челябинска, виновный А. действовал с прямым умыслом, зная, что использование вредоносной программы приведет к наступлению общественно опасных последствий, и желал их наступления.

Мотив и цель являются факультативными признаками субъективной стороны. Отсутствие в диспозиции ст. 273 УК РФ указания на мотив и цель субъективной стороны преступления, предусмотренного данной статьей, является пробелом законодательства. Законодатель устранил этот пробел в последней редакции ч. 2 ст. 273 УК РФ, где в качестве квалифицирующего признака рассматриваемого состава преступления был выделен корыстный мотив: "деяния, предусмотренные частью первой настоящей статьи... совершенные из корыстной заинтересованности". Содержание понятия "корыстная заинтересованность" рассмотрено нами выше при исследовании квалифицирующих признаков неправомерного доступа к охраняемой законом компьютерной информации.

В доктрине уголовного права были предложения включить в диспозицию ст. 273 УК РФ некоторые другие мотивы и цели в качестве квалифицирующих признаков: 1) из хулиганских побуждений; 2) с целью устрашения населения или воздействия на принятие решения органами власти либо международными организациями, а также воспрепятствования нормальной деятельности средств

массовой информации, органов власти, государственных и муниципальных учреждений [56, с. 22-26]; 3) с целью скрыть другое преступление [93, с. 58; 56, с. 22-26 ]; 4) облегчить совершение другого преступления.

Т.М. Лопатина предлагает уточнить редакцию ст. 273 УК РФ введением в диспозицию ч. 1 указания на цель как обязательный признак субъективной стороны состава преступления. В качестве цели ученая предлагает указать несанкционированные уничтожение, блокирование, модификацию либо копирование информации.

# ГЛАВА 3. УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА НАРУШЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ ИЛИ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

## 3.1. ОБЪЕКТИВНЫЕ ПРИЗНАКИ НАРУШЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Состав преступления в соответствии со ст. 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Компьютерные технологии среди прочих средств хранения, переработки и передачи информации являются наиболее удобными и прогрессивными инструментами работы с информацией. Результатом совершения этого преступления считается нарушение нормальной работы технологического оборудования.

Проблема незначительного количества зарегистрированных преступлений по ст. 274 УК РФ [121, с. 13] состоит не только в латентности компьютерных преступлений и отсутствии компьютерной культуры, но и в неудачной формулировке диспозиции ст. 274 УК РФ.

Характеристика общего, родового и видового объектов компьютерных преступлений дана при рассмотрении объекта неправомерного доступа к охраняемой законом компьютерной информации. Мнения ученых о содержании непосредственного объекта ст. 274 УК РФ разделились.

Очень широким, на наш взгляд, является определение непосредственного

объекта анализируемого преступления как общественных отношений в сфере компьютерной информации. В науке существуют следующие более узкие дефиниции непосредственного объекта преступления, предусмотренного ст. 274 УК РФ: установленный порядок эксплуатации ЭВМ, систем ЭВМ или их сети [37, с. 92]; отношения по соблюдению правил эксплуатации аппаратно-технического комплекса [108, с. 46]; общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети.

Как отношения по обеспечению безопасности рассматривают непосредственный объект ст. 274 УК РФ многие правоведы: например, безопасность пользования интеллектуальными и вещественными средствами вычислительной техники; отношения по поводу обеспечения безопасности информационных компьютерных технологий и средств их обеспечения, а также тесно связанных с ними процессов производства, сбора, обработки, накопления, хранения, поиска, передачи, распространения и использования компьютерной информации; общественные отношения в сфере соблюдения установленных правил, обеспечивающих нормальную эксплуатацию ЭВМ, системы ЭВМ или их сети; общественные отношения по обеспечению безопасности компьютерной информации, компьютерных систем и сетей, а также линий связи; общественные отношения, обеспечивающие безопасность информационных систем с точки зрения целостности и конфиденциальности содержащейся в них компьютерной информации [78, с. 88].

Большая часть исследователей относят к предмету преступления охраняемую законом компьютерную информацию. По мнению автора законодатель определил предмет преступления в диспозиции ст. 274 УК РФ. Исследование содержания категории "охраняемая законом компьютерная информация" проведено нами при анализе предмета преступления, предусматривающего ответственность за неправомерный доступ к охраняемой законом компьютерной информации. Непосредственный объект рассматриваемого преступления есть совокупность общественных отношений,

которым преступлением причиняется вред или создается угроза его причинения. Мы придерживаемся мнения, что под непосредственным объектом преступления, предусмотренного ст. 274 УК РФ, следует понимать общественные отношения, обеспечивающие соблюдение установленных обладателем компьютерной информации правил эксплуатации средств ее хранения, обработки или передачи.

Рассматривая объективную сторону отметим, что норма ст. 274 УК РФ является бланкетной, и для определения объективной стороны состава преступления необходимо установить, какие предписания того или иного нормативно-правового акта нарушил виновный. В каждом конкретном случае важно выяснить, какие императивные положения нормативно-правовых актов были нарушены (за невыполнение рекомендательных норм индивид не может быть привлечен к уголовной ответственности). С объективной стороны данное деяние может выражаться как в действии, так и в бездействии виновного, которые проявляются в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям.

Новая редакция ст. 274 УК РФ оперирует такими понятиями, как: средства хранения, обработки или передачи охраняемой законом компьютерной информации; информационно-телекоммуникационные сети; оконченное оборудование.

К средствам хранения, обработки или передачи компьютерной информации И.Р. Бегишев относит персональные компьютеры и иные информационно-телекоммуникационные устройства, в которых компьютерная информация обращается [27, с. 17-18]. К средствам хранения компьютерной информации относятся также карты памяти, USB-флеш-накопители, дискеты, диски и т.п.

Статья 2 ФЗ "Об информации, информационных технологиях и о защите информации" понимает под информационно-телекоммуникационной сетью

технологическую систему, предназначенную для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники. Согласно ст. 2 ФЗ "О связи" [14] оконченное (пользовательское) оборудование - это технические средства для передачи и (или) приема сигналов электросвязи по линиям связи, подключенные к абонентским линиям и находящиеся в пользовании абонентов или предназначенные для таких целей.

Мнения ученых на изменения ст. 274 УК РФ, касающиеся отказа законодателя от перечисления технических средств хранения, обработки и передачи охраняемой законом компьютерной информации, разделились. Например, В.М. Быков и В.Н. Черкасов считают такое решение законодателя правильным. Под компьютерной техникой по его мнению необходимо понимать "электронные устройства, предназначенные для хранения, переработки, передачи информации или осуществления высокотехнологичной связи с неограниченным числом пользователей, если эта техника способна поддерживать программные продукты, созданные для этих целей".

Нарушение правил эксплуатации может выражаться в несоблюдении, ненадлежащем соблюдении, в прямом нарушении установленных правил, обеспечивающих безопасность средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям. Нарушение правил может выражаться в несвоевременном техническом обслуживании узлов и агрегатов, неправильном подключении компьютера к источникам питания, невыполнении резервного копирования, отказе от использования антивирусного программного обеспечения, паролей и иных средств защиты при обработке конфиденциальной компьютерной информации [65]. Понятия "нарушение" и "несоблюдение" правил эксплуатации в контексте данной статьи являются синонимами и могут рассматриваться как равнозначные.

Большинство ученых под такими правилами понимают гигиенические

требования к видеодисплейным терминалам, персональным ЭВМ и организации работы; техническую документацию на приобретаемые компьютеры; конкретные, принимаемые в определенном учреждении или организации, оформленные нормативно и подлежащие доведению до сведения соответствующих работников правила внутреннего распорядка; требования по сертификации компьютерных сетей и оборудования; должностные инструкции конкретных сотрудников; правила пользования компьютерными сетями [108, с. 47].

Перечислим основные документы, за нарушение которых может последовать уголовная ответственность по ст. 274 УК РФ: - ГОСТ Р МЭК 60950-2002 "Безопасность оборудования информационных технологий"; - Санитарно-эпидемиологические правила и нормативы СанПиН 2.2.2/2.4.1340-03 "Гигиенические требования к персональным электронно-вычислительным машинам и организации работы" (в редакции СанПиН 2.2.2/2.4.2198-07. Изменение № 1 к СанПиН 2.2.2/2.4.1340-03) и проч.

Состав преступления, предусмотренный ст. 274 УК РФ, является материальным. Для признания преступления оконченным необходимо наступление одного из следующих последствий, перечисленных в диспозиции нормы: уничтожение, блокирование, модификация либо копирование компьютерной информации. Одновременно эти деяния должны повлечь причинение крупного ущерба. При этом наступившие последствия не должны быть результатом совершения деяний, предусмотренных ст. 272, 273 УК РФ.

Понятия уничтожения, копирования, блокирования, модификации компьютерной информации были проанализированы в настоящей работе ранее.

В соответствии со старой редакцией ст. 274 УК РФ лицо привлекалось к уголовной ответственности, если его действиями причинен существенный ущерб. Доктрина оценивала такую конструкцию как неудачную [114, с. 621]. Существенный вред - это оценочное понятие, которое зависит в каждом конкретном случае от многих показателей.

Факультативные признаки состава преступления не влияют на

квалификацию, но учитываются при индивидуализации наказания. Одним из факультативных признаков любого состава преступления является место совершения преступного деяния. Место совершения нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования либо правил доступа к информационно-телекоммуникационным сетям следует отделять от места наступления общественно опасных последствий. Они могут не совпадать, особенно если нарушаются правила эксплуатации информационно-телекоммуникационных сетей.

Еще одним факультативным признаком преступления является время совершения общественно опасного деяния. Время может не совпадать с временем наступления общественно опасных последствий. Например, общественно опасные последствия при изменении программы могут наступить позже, чем само изменение.

Ученые считают, что преобладающим способом нарушения работы информационно-телекоммуникационных устройств является отказ в обслуживании [27, с. 18]. При отказе в обслуживании уполномоченные пользователи системы не могут получить своевременный доступ к необходимой информации, хотя имеют на это полное право [123, с. 10]. На наш взгляд, отказ в обслуживании не может признаваться способом совершения преступления, предусмотренного ст. 274 УК РФ, так как в этом случае отказ в обслуживании наносит вред автоматизированной системе, а не предмету преступления по ст. 274 УК РФ.

Отметим, что в науке имеет место спор о принципиальной целесообразности криминализации деяний, предусмотренных ст. 274 УК РФ. Например, по мнению Д.В. Добровольского, нет реальной необходимости в криминализации такого отклоняющегося поведения [53, с. 18]. Аналогичной позиции придерживается Т.М. Лопатина, считающая, что данная статья представляет собой пример необоснованной криминализации [83, с. 58].

Ученые, разделяющие эту точку зрения, считают, что на такое поведение можно влиять мерами гражданского и административного права, и предлагают декриминализировать этот состав [60, с. 5-6].

Кроме того, А.В. Суслопаров считает необходимым заменить исследуемый состав преступления на компьютерный саботаж [127, с. 155]. Под компьютерным саботажем он предлагает понимать умышленный ввод, передачу, уничтожение компьютерных данных или компьютерных программ или другое вмешательство в компьютерные системы с целью воспрепятствовать функционированию компьютера или телекоммуникационной системы.

Часть 2 ст. 274 УК РФ устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, причинившее тяжкие последствия или угрозу наступления таковых. Тяжкие последствия вследствие нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети могут выражаться и в смерти человека или причинении тяжкого вреда здоровью потерпевшего, причинении средней тяжести вреда здоровью двум потерпевшим и более, причинении легкого вреда нескольким лицам. К наиболее типичным из них относятся дезорганизация работы юридического лица, уничтожение, блокирование ценной информации, в том числе принадлежащей физическим лицам.

Представляется нецелесообразной декриминализация состава, предусмотренного ст. 274 УК РФ. Действия, входящие в состав объективной стороны преступления, предусмотренного ст. 274 УК РФ, наносят серьезный ущерб обществу и государству, представляя тем самым повышенную общественную опасность. Редкое применение ст. 274 УК РФ на практике не свидетельствует о необходимости ее декриминализации.

## 3.2. СУБЪЕКТИВНЫЕ ПРИЗНАКИ НАРУШЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

В отечественной уголовно-правовой науке нет единого мнения о субъекте преступления, предусмотренного ст. 274 УК РФ. Одни ученые считают, что субъект исследуемого преступления специальный [116, с. 149]. В.В. Воробьев, А.В. Сизов, А.Н. Ягудин исходят из того, что для привлечения лица к уголовной ответственности необходимо установить не только факт наличия у виновного доступа к ЭВМ, системе ЭВМ или их сети, но и факт (задокументированный) прохождения этим лицом инструктажа или ознакомления с правилами эксплуатации. Субъектом преступления является физическое лицо, достигшее 16 лет, имеющее доступ к средствам хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и на которое возложено соблюдение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей и правил доступа к информационно-телекоммуникационным сетям.

В российской уголовно-правовой доктрине существует и противоположное мнение относительно вида субъекта преступления, предусмотренного ч. 1 ст. 274 УК РФ. А.Г. Волеводз справедливо полагает, что субъект анализируемого преступления не специальный, а общий [36, с. 81]. Важно отметить, что Федеральный закон от 7 декабря 2011 г. № 420-ФЗ внес изменения в диспозицию ст. 274 в части определения субъекта преступления и сейчас можно точно утверждать, что субъект данного преступления общий.

Существует точка зрения, что исследуемый состав осуществляется только с прямым умыслом [44, с. 62]. В соответствии с другой позицией нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных

сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям может быть совершено как с прямым, так и с косвенным умыслом [83, с. 32].

Виновный сознает общественно опасный характер нарушения правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, предвидит возможность или неизбежность наступления в результате его действий уничтожения, блокирования, модификации или копирования охраняемой законом компьютерной информации, которые повлекут за собой причинение крупного ущерба, и желает этого (прямой умысел) либо предвидит возможность уничтожения, блокирования, модификации или копирования охраняемой законом компьютерной информации и причинения в результате этого крупного ущерба, однако не желает, но сознательно допускает эти последствия или относится к ним безразлично (косвенный умысел).

Мотив и цель имеют факультативное значение. Но если нарушение правил эксплуатации было произведено с целью совершить иное преступление, то содеянное необходимо квалифицировать по совокупности преступлений [57, с. 95].

Судебная практика показывает, что преступление, предусмотренное ст. 274 УК РФ, совершается с прямым умыслом. Так, например, в соответствии с Постановлением о прекращении уголовного дела от 13 января 2015 г. Лефортовский районный суд г. Москвы установил следующее: органами предварительного следствия А. обвиняется в нарушении правил эксплуатации средств хранения и передачи охраняемой компьютерной информации, повлекшем копирование компьютерной информации, причинившее крупный вред, а именно в том, что он, А., с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ на основании трудового договора №... от ДД.ММ.ГГГГ работал и занимал различные должности в отделе технической поддержки U№IX ООО "ПТ"; согласно

изменению номера к договору от ДД.ММ.ГГГГ А. был переведен на должность ведущего системного администратора U№IX отдела технической поддержки U№IX. ДД.ММ.ГГГГ А. был ознакомлен с должностной инструкцией №... по должности "ведущий системный администратор U№IX", согласно которой ведущий системный администратор U№IX поддерживает в рабочем состоянии программное обеспечение рабочих станций с серверов, обеспечивает своевременное копирование, архивирование и резервирование данных, обеспечивает сетевую безопасность, сохраняет конфиденциальность служебной информации, которая была им изучена и собственноручно подписана. В период времени с ДД.ММ.ГГГГ по ДД.ММ.ГГГГ (точное время следствием не установлено) А., имея умысел на нарушение правил эксплуатации средств хранения, передачи охраняемой компьютерной информации, повлекшее копирование компьютерной информации, находясь на своем рабочем месте, предоставленном ООО "ПТ", используя средства авторизации (логин и пароль), предоставленные ООО "ПТ", и имея в силу исполняемых обязанностей доступ к информационным носителям, на которых содержится охраняемая компьютерная информация, и действуя в нарушение закона, скопировал на USB-носитель информацию из базы данных ООО "ПТ" [163].

Автор полагает, что нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование охраняемой законом компьютерной информации, совершается с прямым умыслом.

# ЗАКЛЮЧЕНИЕ

Сфера обмена и обработки компьютерной информации играет все большую роль в процессах развития российского общества, а криминальные проявления в этой сфере приобретают все большие масштабы. Это предопределяет необходимость охвата ее регулятивными и охранительными функциями права, а также повышает внимание к информационной безопасности как отдельной составляющей национальной безопасности России. В таких условиях важным является системный подход к формированию понятийно-терминологического аппарата безопасного обращения компьютерной информации, который обеспечит ее адекватное содержательное наполнение, соответствие требованиям, предъявляемым к правовой терминологии, а также гармонизацию с традициями русского уголовного права и терминологией действующего уголовного законодательства.

Рассмотренные при написании диссертации вопросы могут быть использованы в целях совершенствования судебно-следственной практики и разработки теоретических положений уголовно-правовой науки.

Результаты данного исследования можно свести к следующим основным положениям.

1. Несмотря на то, что информационная безопасность традиционно ассоциируется главным образом с компьютерными технологиями и совершаемыми в этой сфере правонарушениями, значительное количество статей УК РФ направлено на защиту иных отношений, в которых использование компьютерной техники и информационных технологий не предполагается либо такое использование не является определяющим. Речь идет об обеспечении сохранности различных видов тайны (личной, государственной), обеспечении неприкосновенности частной жизни, а также чести и достоинства человека и гражданина, об обеспечении права на доступ к информации, права на комфортную информационную среду, не посягающую на мораль, нравственность, психологический комфорт личности.

2. С учетом теоретических подходов и сложившейся практики сформулированы основные, значимые для квалификации преступлений в сфере компьютерной информации понятия, такие как: неправомерный доступ, блокирование, уничтожение, копирование, модификация информации, вредоносная программа, технические средства, программные средства, средства хранения, обработки или передачи компьютерной информации и прочее.

3. Сделан вывод о том, что требуется на уровне Постановлений Пленума Верховного Суда Российской Федерации разъяснить ряд вышеуказанных и других специальных понятий, в то время как диспозиции статей, предусмотренных гл. 28 УК РФ нецелесообразно еще больше «нагружать» специальной терминологией, так как это вызовет трудности в правоприменительной практике.

4. Преступления против компьютерной информации имеют свои специфические черты, которые оказывают существенное влияние на особенности криминальной, а также криминалистической деятельности. Такими чертами являются: место совершения преступления, носящее трансграничный характер, технологии, позволяющие в кратчайшие сроки «замести» следы преступления, терминологическая загруженность и прочее.

5. Преступления в сфере компьютерной информации зачастую граничат с преступлениями против собственности и иных направленностей, ввиду чего особую значимость приобретает установление направленности преступного умысла при их расследовании и рассмотрении судами.

6. С позиций совершенствования уголовного законодательства считает целесообразным введение в УК РФ ст. 272.1 «Незаконное завладение ЭВМ или иным машинным носителем компьютерной информации без цели хищения для осуществления неправомерного доступа к компьютерной информации».

# БИБЛИОГРАФИЧЕСКИЙ СПИСОК

## 1. НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ


1. Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 г. // Российская газета. - 1993. - № 237.
2. Гражданский кодекс Российской Федерации. URL.: http://base.gara№t.ru/10164072/ (дата обращения: 23.09.2019).
3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. URL.: http://zako№base.ru/ugolov№yj-kodeks (дата обращения: 23.09.2019).
4. Уголовный кодекс Республики Беларусь от 9 июля 1999 г. № 275-З. URL.: http://etalo№li№e.by/?type=text&reg№um=HK9900275#load_text_№o№e_1_ (дата обращения: 23.09.2019).
5. Федеральный закон от 21 ноября 2011 г. № 323-ФЗ "Об основах охраны здоровья граждан в Российской Федерации" // Российская газета. № 263. 23.11.2011.
6. Федеральный закон от 27 июля 2006 г. № 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.
7. Федеральный закон от 20 августа 2004 г. № 119-ФЗ "О государственной защите потерпевших, свидетелей и иных участников уголовного судопроизводства" // Собрание законодательства Российской Федерации. 2004. № 34. Ст. 3534.
8. Федеральный закон от 29 июля 2004 г. № 98-ФЗ "О коммерческой тайне" // Собрание законодательства Российской Федерации. 2004. № 32. Ст. 3283.
9. Федеральный закон от 15 ноября 1997 г. № 143-ФЗ "Об актах гражданского состояния" // Собрание законодательства Российской Федерации. 1997. № 47. Ст. 5340.
10. Федеральный закон от 21 июля 1993 г. № 5485-1 "О государственной

тайне" // Собрание законодательства Российской Федерации. 1997. № 41. Ст. 4673.

11. Основы законодательства Российской Федерации о нотариате от 11 февраля 1993 г. № 4462-1 // Российская газета. 13.03.1993.
12. Федеральный закон от 31 мая 2002 г. № 63-ФЗ "Об адвокатской деятельности и адвокатуре в Российской Федерации" // Собрание законодательства Российской Федерации. 2002. № 23. Ст. 2102.
13. Федеральный закон от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации" URL.: http://base.garа№t.ru/12148555/#ixzz3IH№T2E7K (дата обращения: 23.09.2019).
14. Федеральный закон от 7 июля 2003 г. № 126-ФЗ "О связи". URL.: http://www.co№sulta№t.ru/popular/commu№icatio№/.
15. Указ Президента РФ от 6 марта 1997 г. № 188 "Об утверждении Перечня сведений конфиденциального характера" // Собрание законодательства Российской Федерации. 1997. № 10. Ст. 1127.
16. Постановление Правительства РФ от 3 февраля 2012 г. № 79 "О лицензировании деятельности по технической защите конфиденциальной информации" // Собрание законодательства Российской Федерации. 2012. № 7. Ст. 863.
17. Постановление Правительства РФ от 10 сентября 2007 г. № 575 "Об утверждении Правил оказания телематических услуг связи" // Собрание законодательства Российской Федерации. 2007. № 38. Ст. 4552.
18. Положение о сертификации средств защиты информации (утв. Постановлением Правительства РФ от 26 июня 1995 г. № 608) // Собрание законодательства Российской Федерации. 1995. № 27. Ст. 2579.

## 2. НАУЧНАЯ И УЧЕБНАЯ ЛИТЕРАТУРА

19. Абов А.И. Преступления в сфере компьютерной информации:

неправомерный доступ к компьютерной информации. М.: Прима Пресс, 2002. 25 с.

20. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. М.: Мир, 1999. 352 с.
21. Айсанов Р.М. Состав неправомерного доступа к компьютерной информации в российском, международном и зарубежном уголовном законодательстве: Дис. ... канд. юрид. наук. М., 2006. 192 с.
22. Алескеров В.И., Максименко И.А. Уголовно-правовая и криминалистическая характеристика современных видов преступлений: Лекция. Домодедово: ВИПК МВД России, 2011. 26 с.
23. Анисимова И.А. Уголовно-правовое значение преступного вреда: Дис. ... канд. юрид. наук. Томск, 2008. 232 с.
24. Батурин Ю.М. Право и политика в компьютерном округе. М., 1987. 116 с.
25. Бачило И.Л. Информационное право. Основы практической информатики: Учеб. пособие. М.: Юринформцентр, 2001. 352 с.
26. Бойцов А.И. Преступления в сфере компьютерной информации // Уголовное право России. Особенная часть: Учебник для вузов / Под ред. Н.М. Кропачева и др. СПб.: Университетский издательский консорциум "Юридическая книга", 2010. 1624 с.
27. Бородин А.В. Феномен компьютерных вирусов: элементы теории и экономика существования. Йошкар-Ола: Марийский государственный технический университет, 2004. 144 с.
28. Борчева Н.А. Компьютерные преступления в России. Комментарий к Уголовному кодексу Российской Федерации. М.: Собрание, 2004. 224 с.
29. Бражник С.Д. Актуальные проблемы совершенствования законодательства в сфере компьютерной информации: Монография. Ярославль: МУБиНТ, 2007. 159 с.
30. Бражник С.Д. Преступления в сфере компьютерной информации: проблемы законодательной техники: Дис. ... канд. юрид. наук. Ижевск, 2002. 189 с.

31. Буз С.А. Уголовно-правовые средства борьбы с преступлениями в сфере компьютерной информации. Краснодар, 2002. 134 с.
32. Букалерова Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы: Автореф. дис. ... д-ра юрид. наук. М., 2007. 574 с.
33. Быстряков Е.Н. Расследование компьютерных преступлений. Саратов: СГАП, 2000. 92 с.
34. Бытко С.Ю. Преступления в сфере компьютерной информации: Учеб. пособие для студентов юридических специальностей. Саратов: Изд-во Саратовского университета, 2004. 49 с.
35. Васильев Н.В. Принципы советского уголовного права: Учеб. пособие. М., 1983. 60 с.
36. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М.: Юрлитинформ, 2002. 496 с.
37. Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис. ... канд. юрид. наук. Н. Новгород, 2000. 201 с.
38. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: Учеб. пособие / Под ред. проф. Н.Г. Шурухнова. М.: ЮИ МВД РФ; Книжный мир, 2001. 88 с.
39. Гаврилин Ю.В. Расследование преступлений, посягающих на информационную безопасность в сфере экономики: теоретические, организационно-тактические и методические основы: Дис. ... д-ра юрид. наук. М., 2009. 187 с.
40. Гаврилов О.А. Информатизация правовой системы России. Теоретические и практические проблемы: Учеб. пособие. М.: Юридическая книга, 1998. 144 с.
41. Гайдамакин А.А. Информационная безопасность в органах внутренних

дел и применение информационных технологий в борьбе с преступностью. Омск, 2010. 118 с.

42. Галиакбаров Р.Р. Уголовное право. Общая часть: Учебник. Краснодар, 1999. 445 с.
43. Гаухман Л.Д. Уголовная ответственность за организацию преступного сообщества. М., 1997. 213 с.
44. Геллер А.В. Уголовно-правовые и криминологические аспекты обеспечения защиты информации и Интернета: Дис. ... канд. юрид. наук. М., 2006. 219 с.
45. Городов О.А. Основы информационного права России: Учеб. пособие. СПб.: Юрид. центр "Пресс", 2003. 305 с.
46. Григоренко С.В. Преступления в сфере компьютерной информации. М.: ПОЛТЕКС, 2003. 39 с.
47. Гусев А.Н. Комментарий к Уголовному кодексу. М.: Экзамен, 2006. 564 с.
48. Дагель П.С. Субъективная сторона преступления и ее установление. Воронеж, 1974. 218 с.
49. Даль В. Толковый словарь живого великорусского языка. М.: Терра, 1995.
50. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование): Дис. ... канд. юрид. наук. Волгоград, 2005. 193 с.
51. Дворецкий М.Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации. Тамбов: Изд-во ТГУ им. Г.Р. Державина, 2005. 474 с.
52. Дворецкий М.Ю. Преступления в сфере компьютерной информации: понятие, система, проблемы квалификации и наказания: Монография. Тамбов: Изд-во ТГУ, 2003. 197 с.
53. Добровольский Д.В. Актуальные проблемы борьбы с преступностью (уголовно-правовые и криминологические проблемы): Дис. ... канд. юрид. наук. М., 2005. 218 с.

54. Дубягина О.П. Криминологическая характеристика норм обычаев и средств коммуникации криминальной среды: Автореф. ... канд. юрид. наук. М., 2008. 26 с.
55. Евдокимов В.Б., Михайленко К.Е. Международная правовая помощь по гражданским и уголовным делам: на примере стран СНГ. М.: Олма-Пресс, 2004. 384 с.
56. Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия неправомерному доступу к компьютерной информации (по материалам Восточно-Сибирского региона): Дис. ... канд. юрид. наук. Иркутск, 2006. 203 с.
57. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Дис. ... канд. юрид. наук. М., 2007. 160 с.
58. Золотухин С.Н. Уголовно-правовые и криминологические аспекты преступлений в сфере компьютерной информации: Учеб. пособие. Краснодар, 2008. 137 с.
59. Иванова И.Г. Выявление и расследование неправомерного доступа к компьютерной информации: Дис. ... канд. юрид. наук. Красноярск, 2007. 197 с.
60. Кабанова А.Ж. Преступления в сфере компьютерной информации (уголовно-правовые и криминологические аспекты): Автореф. дис. ... канд. юрид. наук. Ростов н/Д, 2004. 24 с.
61. Карпов В.С. Уголовная ответственность за преступления в сфере компьютерной информации: Дис. ... канд. юрид. наук. Красноярск, 2002. 209 с.
62. Каспаров А.А. Создание, использование и распространение вредоносных программ для ЭВМ: уголовно-правовые аспекты. М.: ТИССО, 2003. 40 с.
63. Клепицкий И.А. Преступления в сфере компьютерной информации // Уголовное право Российской Федерации. Особенная часть: Учебник / Под ред. Б.В. Здравомилова; 2-е изд., перераб. и доп. М.: ИНФРА-М,

2000. 352 с.

64. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Отв. ред. В.М. Лебедев. 13-е изд., перераб. и доп. М.: Юрайт, 2013. 1069 с.
65. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. А.И. Чучаева. URL.: http://www.co№sulta№t.ru/ (дата обращения: 23.09.2019)..
66. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / Под ред. А.А. Чекалина, В.Т. Томина, В.В. Сверчкова. URL.: http://www.co№sulta№t.ru/ (дата обращения: 23.09.2019)..
67. Комментарий к Уголовному кодексу Российской Федерации / Отв. ред. А.В. Наумов. М.: Юристъ, 1996. 824 с.
68. Комментарий к Уголовному кодексу Российской Федерации / Под общ. ред. Ю.И. Скуратова и В.М. Лебедева. М.: ИНФРА-М-Норма, 1996. 592 с.
69. Комментарий к Уголовному кодексу Российской Федерации / Под ред. О.Ф. Шишова. М., 1998. 628 с.
70. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.И. Радченко, А.С. Михлина. СПб.: Питер, 2007. 872 с.
71. Комментарий к Уголовному кодексу Российской Федерации / Ю.В. Белянинова, А.М. Дедов, А.А Дедов и др.; Под ред. А.Г. Королькова. М.: ЭКСМО, 2004. 1120 с.
72. Комментарий к Уголовному кодексу Российской Федерации. С постатейными материалами и практическими разъяснениями / А.Б. Борисов. М., 2008. 1072 с.
73. Комментарий к Уголовному кодексу Российской Федерации: расширенный уголовно-правовой анализ с материалами судебно-следственной практики / О.Я. Баев, Р.А. Базаров, А.В. Борбат и др.; Под общ. ред. А.П. Новикова. М.: Экзамен, 2006. 976 с.
74. Копырюлин А.Н. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический аспекты: Дис. ... канд. юрид.

наук. Тамбов, 2007. 242 с.

75. Кочои С.М. Ответственность за корыстные преступления против собственности по законодательству России: Дис. ... д-ра юрид. наук. М., 1998. 343 с.
76. Криминология. Особенная часть. В 2 т. Т. 2: Учебник для академ. бакалавриата / Под ред. О.С. Капинус. М.: Изд-во "Юрайт", 2016. С. 241.
77. Криминология: Учебник / Под ред. В.Н. Кудрявцева, В.Е. Эминова. М.: Юристъ, 2000. 678 с.
78. Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: Дис. ... д-ра юрид. наук. М., 1998. 334 с.
79. Крылов В.В. Расследование преступлений в сфере информации. М.: Городец, 1998. 264 с.
80. Кудрявцев В.Н. Объективная сторона преступления. М.: Госюриздат, 1960. 193 с.
81. Кузнецов П.У. Теоретические основания информационного права: Дис. ... д-ра юрид. наук. Екатеринбург, 2005. 410 с.
82. Курушин В.Д., Минаев В.А. Справочник. Компьютерные преступления и безопасность. М.: Новый юрист, 1998. 256 с.
83. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: Дис. ... д-ра юрид. наук. М., 2006. 418 с.
84. Ляпунов Ю.И. Общественная опасность деяния как универсальная категория советского уголовного права: Учеб. пособие. М.: Издательство ВЮЗШ МВД СССР, 1989. 119 с.
85. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: Учеб.-практ. пособие. М.: Палеотип; Логос, 2002. 148 с.
86. Мазуров В.А. Тайна: государственная, коммерческая, банковская, частной жизни. Уголовно-правовая защита: Учеб. пособие. М.: Дашков и Ко, 2003. 156 с.

87. Максимов В.Ю. Компьютерные преступления (вирусный аспект). Ставрополь: Ставроп. кн. изд-во, 1999. 112 с.
88. Максимов В.Ю. Незаконное обращение с вредоносными компьютерными программами для ЭВМ: проблемы криминализации, дифференциации ответственности и индивидуализации наказания: Дис. ... канд. юрид. наук. Краснодар, 1998. 169 с.
89. Малыковцев М.М. Уголовная ответственность за создание, использование и распространение вредоносных программ для ЭВМ: Автореф. дис. ... канд. юрид. наук. М., 2006. 24 с.
90. Малышенко Д.Г. Уголовная ответственность за неправомерный доступ к компьютерной информации: Дис. ... канд. юрид. наук. М., 2002. 166 с.
91. Маслакова Е.А. Незаконный оборот вредоносных компьютерных программ: уголовно-правовые и криминологические аспекты: Дис. ... канд. юрид. наук. М., 2008. 198 с.
92. Медведовский И.Д. Атака на I№ter№et. М.: ДМК-Пресс, 1999. 42 с.
93. Менжега М.М. Методика расследования создания и использования вредоносных программ для ЭВМ. М.: Юрлитинформ, 2009. 180 с.
94. Мешков В.М. Компьютерные преступления и защита компьютерной информации: Науч.-практ. пособие. Калининград: Изд-во Калинингр. ЮИ МВД России, 2003. 120 с.
95. Мещеряков В.А. Преступления в сфере компьютерной информации: правовой и криминалистический анализ. Воронеж: ВГУ, 2001. 176 с.
96. Наумов А.В. Российское уголовное право. Общая часть. Курс лекций. М.: БЕК, 1996. 560 с.
97. Научно-практический комментарий к Уголовному кодексу Российской Федерации. В 2 т. Т. 2 / Под ред. Н.Н. Панченко. Н. Новгород, 1996. С. 641.
98. Никифоров Б.С. Объект преступления по советскому уголовному праву. М.: Госюриздат, 1960. 228 с.
99. Новая философская энциклопедия. В 4 т. Т. 1. М.: Мысль, 2010. 744 с.

100. Новое уголовное право России. Особенная часть: Учеб. пособие / Г.Н. Борзенков, С.В. Бородин, Б.В. Волженкин, В.С. Комиссаров и др.; под ред. Н.Ф. Кузнецовой. М.: Зерцало; ТЕИС, 1996. 391 с.
101. Ожегов С.И. Словарь русского языка / Под ред. Н.Ю. Шведовой. 23-е изд., испр. М.: Русский язык, 1990. 917 с.
102. Озерский С.В. Компьютерные преступления: методы противодействия и защиты информации: Учеб. пособие. Саратов: Саратов. юрид. институт МВД России, 2004. 114 с.
103. Осипенко А.Л. Борьба с преступностью в глобальных сетях: международный опыт: Монография. М.: Норма, 2004. 432 с.
104. Павлов В.Г. Субъект преступления. СПб.: Юридический центр "Пресс", 2001. 318 с.
105. Павлов В.Г. Субъект преступления: История, теория и практика: Дис. ... д-ра юрид. наук. СПб., 2000. 405 с.
106. Панфилова Е.И. Компьютерные преступления / Е.И. Панфилова, А.Н. Попов; Науч. ред. проф. Б.В. Волженкин. СПб.: Изд-во СПб. юрид. ин-та Генпрокуратуры РФ, 2003. 48 с.
107. Парфенов А.Ф. Общее учение об объективной стороне преступления Дис. ... канд. юрид. наук. СПб., 2004. 428 с.
108. Преступления в сфере компьютерной информации: квалификация и доказывание: Учеб. пособие / Под ред. Ю.В. Гаврилина. М.: ЮИ МВД РФ, 2003. 245 с.
109. Пущин В.С. Преступления в сфере компьютерной информации. М., 2000. 168 с.
110. Расследование преступлений повышенной общественной опасности / Под ред. Н.А. Селиванова, А.И. Дворкина. М., 1998. 82 с.
111. Ратникова А.Е. Уголовно-правовое обеспечение права на информацию (Сравнительно-правовое исследование): Автореф. дис. ... канд. юрид. наук. М., 2006. 25 с.
112. Российская интернет-аудитория является крупнейшей в Европе. URL.:

http://www.gazeta.ru/tech/№ews/2015/12/22/№8043815.shtml. (дата обращения: 23.09.2019).

113. Российское уголовное право. Общая часть / Под ред. В.С. Комиссарова. СПб.: Питер, 2005. 560 с.
114. Российское уголовное право. Особенная часть / Под ред. А.И. Рарога. М., 2001. 479 с.
115. Российское уголовное право. Особенная часть / Под ред. В.Н. Кудрявцева, А.В. Наумова. М.: Юристъ, 1997. 496 с.
116. Российское уголовное право. Особенная часть / Под ред. Л.В. Иногамовой-Хегай, В.С. Комиссарова, А.И. Рарога. М., 2006. 472 с.
117. Сало И.А. Преступные действия с компьютерной информацией ограниченного доступа: Дис. ... канд. юрид. наук. М., 2011. 285 с.
118. Смирнова Т.Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Дис. ... канд. юрид. наук. М., 1998. 161 с.
119. Снытников А.А. Обеспечение и защита права на информацию / А.А. Снытников, Л.В. Туманова. М.: Городец-издат, 2001. 344 с.
120. Советский энциклопедический словарь / Под ред. А.М. Прохорова. М., 1984. 1600 с.
121. Спирина С.Г. Криминологические и уголовно-правовые проблемы в сфере компьютерной информации: Автореф. дис. ... канд. юрид. наук. Краснодар, 2001. 216 с.
122. Старичков М.В. Умышленные преступления в сфере компьютерной информации: уголовно-правовая и криминологическая характеристики: Дис. ... канд. юрид. наук. Иркутск, 2006. 237 с.
123. Струков В.И. Правовое обеспечение защиты информации: Учеб.-метод. пособие. Ч. 2. Таганрог: ТТИ ЮФУ, 2008. 48 с.
124. Стяжкина С.А. Гарантии прав и законных интересов несовершеннолетних в институте наказания: Автореф. дис. ... канд. юрид. наук. Ижевск, 2006. 23 с.
125. Сударева Л.А. Правовое и информационное обеспечение деятельности

органов внутренних дел по предупреждению компьютерных преступлений: Дис. ... канд. юрид. наук. М., 2008. 250 с.

126. Суслопаров А.В. Информационные преступления: Дис. ... канд. юрид. наук. Красноярск, 2008. 249 с.
127. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера: Дис. ... канд. юрид. наук. Владивосток, 2010. 206 с.
128. Толковый словарь Д.Н. Ушакова. URL.: http://e№c-dic.com/sy№o№ym/Modificirovat-85218.html (дата обращения: 23.09.2019).
129. Трахов А.И. Уголовный закон в теории и судебной практике. Майкоп, 2001. 304 с.
130. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: Дис. ... канд. юрид. наук. Владивосток, 2005. 235 с.
131. Уголовное право России. Часть Особенная: Учебник для вузов / Отв. ред. Л.Л. Кругликов. М.: Волтерс Клувер, 2005. 839 с.
132. Уголовное право Российской Федерации. Особенная часть / Под ред. Б.В. Здравомыслова. М.: Юристъ, 1996. 559 с.
133. Уголовное право. Особенная часть / Под ред. И.Я. Козаченко, З.А. Незнамовой, Г.П. Новоселова. М.: Норма, 2001. 960 с.
134. Уголовное право. Особенная часть / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. М., 1998. 381 с.
135. Уголовное право. Особенная часть. Учебник / Под ред. Ф.Р. Сундурова, М.В. Талан. М., 2012. 518 с.
136. Уголовное право. Особенная часть: Конспект лекций / М.М. Смирнов, А.П. Толмачев. М.: Приор, 2002. 336 с.
137. Уголовное право. Особенная часть: Учебник / Под ред. В.Н. Петрашова. М., 1999. 420 с.
138. Уголовное право. Особенная часть: Учебник для вузов / Отв. ред. И.Я.

Козаченко, З.А. Незнамова, Г.П. Новоселов. М.: ИНФРА-М, 1998. 768 с.

139. Ушаков С.И. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика): Дис. ... канд. юрид. наук. Ростов н/Д, 2000. 176 с.
140. Фролов Е.А. Объект уголовно-правовой охраны и его роль в организации борьбы с посягательствами на социалистическую собственность: Автореф. дис. ... д-ра юрид. наук. Свердловск, 1971. 421 с.
141. Числин В.П. Уголовно-правовые меры защиты информации от неправомерного доступа: Дис. ... канд. юрид. наук. М., 2004. 134 с.
142. Ягудин А.Н. Уголовная ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей: Дис. ... канд. юрид. наук. М., 2012. 201 с.

## 3. МАТЕРИАЛЫ ПРАКТИКИ

143. Постановление Пленума Верховного Суда РФ от 16 октября 2009 г. № 19 "О судебной практике по делам о злоупотреблении должностными полномочиями и о превышении должностных полномочий" // Бюллетень Верховного суда Российской Федерации. 2009. № 12.
144. Постановление президиума Свердловского областного суда от 30 сентября 2009 г. по делу № 44-У-86/2009. URL.: http://base.co№sulta№t.ru/co№s/cgi/o№li№e.cgi?req=doc;base=RASVR;№=40415div=LAW;mb=LAW;opt=I;ts=4C6C471BB1419447623925A24E559475;md=0.8729100401515647 (дата обращения: 23.09.2019).
145. Кассационное определение от 26 апреля 2012 г. по делу № 22-475/2012 судебной коллегии по уголовным делам суда Ямало-Ненецкого автономного округа. URL.: http://rospravosudie.com/court-sud-yamalo-№e№eckogo-avto№om№ogo-okruga-yamalo-№e№eckij-avto№om№yj-okrug-s/act-1047173104 (дата обращения: 23.09.2019).

146. Приговор Октябрьского районного суда г. Самары от 16 июля 2009 г. // Архив районного суда г. Самары.
147. Приговор Вязнинковского городского суда Владимирской области от 11 октября 2011 г. по делу № 1-301/2011. URL.: http://docs.pravo.ru/docume№t/view/37483892/?mode=full (дата обращения: 23.09.2019).
148. Приговор Железнодорожного районного суда г. Пензы от 14 апреля 2011 г. по делу № 1-128/11. URL.: http://zhelez№odorozh№ii.p№z.sudrf.ru/ (дата обращения: 23.09.2019).
149. Приговор Басманного районного суда г. Москвы от 12 июля 2011 г. по уголовному делу № 1-190/11. URL.: http://rospravosudie.com/court-basma№№yj-rajo№№yj-sud-gorod-moskva-s/act-100509598/ (дата обращения: 23.09.2019).
150. Приговор Автозаводского районного суда г. Тольятти Самарской области от 19 марта 2010 г. по уголовному делу № 1-480/10 (бумажный носитель).
151. Приговор Ленинского районного суда г. Пензы от 22 ноября 2010 г. по делу № 1-188/10. URL.: https://rospravosudie.com/court-kame№skij-gorodskoj-sud-pe№ze№skaya-oblast-s/ (дата обращения: 23.09.2019).
152. Приговор Советского районного суда г. Томска от 14 октября 2010 г. URL.: http://sovetsky.tms.sudrf.ru/modules.php?№ame=bsr&op=pri№t_text&cl=l&id=706000410120809375970310001734l3 (дата обращения: 23.09.2019).
153. Приговор Тавдинского районного суда Свердловской области от 5 апреля 2011 г. URL.: http://tavdi№sky.svd.sudrf.ru/modules.php?№ame=documsud&id=808 (дата обращения: 23.09.2019).
154. Приговор Индустриального суда г. Ижевска от 9 июня 2011 г. URL.: http://rospravosudie.com/court-i№dustrial№yj-rajo№№yj-sud-g-izhevska-dmurtskaya-respublika-s/act-100416500 (дата обращения: 23.09.2019).
155. Приговор Каменского городского суда Пензенской области от 11 апреля

2011 г. по делу № 1-51/2011. URL.: https://rospravosudie.com/court-kame№skij-gorodskoj-sud-pe№ze№skaya-oblast-s/ (дата обращения: 23.09.2019).

156. Приговор Ленинского районного суда г. Тюмени от 17 июля 2012 г. по уголовному делу № 1-619/2012. URL.: http://www.gcourts.ru/case/10110350 (дата обращения: 23.09.2019).
157. Приговор Ленинского районного суда г. Курска от 12 мая 2012 г. по уголовному делу № 1-81/7-2012. URL.: http://actoscope.com/cfo/kurskobl/le№sud-krs/ug/1/prigovor-po-st-272-chl-uk-rf21062012-4637783/ (дата обращения: 23.09.2019).
158. Приговор Чкаловского районного суда г. Екатеринбурга от 13 октября 2011 г. по делу № 1-749/2011. URL.: https://rospravosudie.com/court-chkalovskij-rajo№№yj-sud-g-ekateri№burga-sverdlovskaya-oblast-s/act-103444196 (дата обращения: 23.09.2019).
159. Приговор Тракторозаводского районного суда г. Челябинска по делу № 1-125/2010. URL.: https://rospravosudie.com/court-alatyrskij-rajo№№yj-sud-chuvashskaya-respublika-s/act-100050559 (дата обращения: 23.09.2019).
160. Приговор Новочеркасского городского суда Ростовской области от 10 апреля 2013 г. URL.: http://rospravosudie.com (дата обращения: 23.09.2019).
161. Постановление Первомайского районного суда г. Ижевска от 14 марта 2012 г. о прекращении уголовного дела № 1-155/12.
162. Постановление Первомайского районного суда г. Ижевска от 22 марта 2012 г. о прекращении уголовного дела № 1-162/12.
163. Постановление Лефортовского районного суда г. Москвы от 13 января 2015 г. о прекращении уголовного дела. URL.: https://rospravosudie.com/court-lefortovskij-rajo№№yj-sud-gorod-moskva-s/act-470253221/ (дата обращения: 23.09.2019).