РЕФЕРАТ

Тема выпускной квалификационной работы: Преступления в сфере компьютерной информации (по отдельным составам).

Актуальность темы «Преступления в сфере компьютерной информации» обусловлена стремительным развитием информационных технологий и их проникновением во все сферы жизни общества. С каждым годом количество преступлений, связанных с использованием компьютеров и интернета, увеличивается, что вызывает необходимость глубокого изучения данной проблематики.

Компьютерные преступления представляют собой серьёзную угрозу для национальной безопасности, экономической стабильности и прав человека. Они включают в себя широкий спектр деяний, начиная от несанкционированного доступа к информации и заканчивая разработкой и распространением вредоносного программного обеспечения.

Актуальность темы обусловлена также необходимостью разработки эффективных мер противодействия компьютерным преступлениям. Это требует комплексного подхода, включающего законодательные, организационные и технические меры. Необходимо совершенствовать законодательство в области информационной безопасности, повышать квалификацию специалистов в области информационных технологий и развивать международное сотрудничество в борьбе с киберпреступностью.

Кроме того, актуальность темы связана с постоянным изменением методов и средств совершения компьютерных преступлений. Киберпреступники постоянно разрабатывают новые способы обхода систем защиты и нанесения ущерба. Это требует постоянного мониторинга ситуации и адаптации мер противодействия к новым вызовам.

Цель работы состоит в проведении комплексного уголовно-правового и криминологического исследования состояния, тенденций и особенностей преступлений в сфере компьютерной информации в Российской Федерации.

В рамках исследования необходимо решить следующие задачи:

1. Проанализировать правовые нормы, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации.
2. Исследовать проблемы, возникающие при квалификации таких преступлений, и сложности с привлечением к уголовной ответственности.
3. Изучить специфику и проблемы, связанные с раскрытием и расследованием преступлений в данной сфере.

Преступления в сфере информационных технологий включают в себя множество действий, таких как распространение вредоносного программного обеспечения, взлом паролей, кража личных данных, фишинг, распространение незаконной информации через интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем. Эти действия могут привести к нарушению работы автоматизированных систем управления и контроля, серьёзным сбоям в работе компьютеров и их систем, несанкционированным действиям по уничтожению, изменению, искажению, копированию информации и информационных ресурсов.

История преступлений в сфере информационных технологий в России началась в конце 70-х годов XX века, когда информационные технологии стали активно распространяться. Первое известное преступление в этой сфере было совершено в 1979 году в Вильнюсе на сумму 80 тысяч рублей. В 1991 году в России произошло одно из первых крупных компьютерных преступлений, связанное с хищением на сумму 125,5 тысяч долларов США и подготовкой к хищению ещё свыше 500 тысяч долларов США во Внешэкономбанке СССР.

В 1996 году был принят Уголовный кодекс Российской Федерации, который содержал отдельную главу, посвящённую уголовной ответственности за преступления в сфере компьютерной информации. Эта глава практически полностью повторяла нормативные положения Модельного кодекса стран — участниц СНГ, принятого в том же году.

С тех пор наблюдается рост числа преступлений в сфере компьютерной информации, что связано с увеличением количества пользователей интернета и развитием информационных технологий.

Преступления в сфере компьютерной информации, описанные в главе 28 Уголовного кодекса Российской Федерации, включают в себя неправомерный доступ к компьютерной информации (статья 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (статья 273 УК РФ), нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно телекоммуникационных сетей (статья 274 УК РФ), а также неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (статья 274-1 УК РФ).

Объекты преступлений в сфере компьютерной информации включают в себя охраняемую законом компьютерную информацию, средства хранения, обработки или передачи компьютерной информации, а также критическую информационную инфраструктуру Российской Федерации.

Субъектами преступлений могут быть физические лица, достигшие возраста уголовной ответственности (обычно 16 лет), которые совершают действия, предусмотренные соответствующими статьями УК РФ.

Предметами преступлений являются компьютерная информация, вредоносные компьютерные программы, а также средства хранения, обработки или передачи компьютерной информации.

Ответственность за преступления в сфере компьютерной информации может включать в себя штрафы, исправительные работы, лишение свободы на различные сроки в зависимости от тяжести совершенного преступления и его последствий. Например, за неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации, лицо может понести наказание в виде штрафа в размере до 200 тысяч рублей, исправительных работ – до 1 года или лишения свободы до 2 лет.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В последние десятилетия мир претерпел значительные изменения благодаря открытиям в различных областях науки, развитию информационно-коммуникационных технологий и технологическому обновлению промышленности. Эти достижения привели к формированию информационного общества, основой которого являются процессы создания, обработки, хранения и использования информации в различных сферах человеческой деятельности. Эти процессы играют ключевую роль в современном обществе и продолжают влиять на его развитие.

Информационное общество характеризуется высокой степенью зависимости от информации и информационных технологий. Оно предполагает наличие развитой инфраструктуры для создания, обработки, хранения и распространения информации, а также высокий уровень информационной культуры населения. Это позволяет эффективно использовать информацию для принятия обоснованных решений, повышения качества жизни и развития экономики.

Однако, несмотря на многочисленные преимущества, которые предоставляет информационное общество, оно также привело к возникновению новых видов преступлений, связанных с компьютерной информацией. Эти преступления отличаются специфическими методами совершения, способами сокрытия следов и имеют высокую степень латентности, что затрудняет их раскрытие.

Хотя было проведено множество исследований, многие вопросы всё ещё вызывают споры или остаются нерешёнными. Кроме того, с появлением новых технологий изменяются способы совершения преступлений в сфере компьютерной информации. Возникают новые методы сокрытия как самих незаконных действий, так и улик, указывающих на преступников. Поэтому необходимо постоянное научное внимание к проблеме обнаружения и

расследования таких преступлений, а также глубокие знания в области информационных технологий у специалистов, занимающихся этой работой.

Недостаточная изученность неправомерного доступа к компьютерной информации в контексте криминологии, необходимость совершенствования уголовного законодательства и значимость комплексного анализа правовых и организационных мер предотвращения и пресечения таких правонарушений определили выбор темы дипломной работы.

Объектом исследования данной работы являются общественные отношения, в части неправомерного использования компьютерной информации и информационных ресурсов.

Предмет исследования включает в себя: преступность в сфере компьютерной информации, как объект уголовно-правового регулирования, её состояние, структуру и динамику; методы, особенности расследования преступлений в сфере компьютерной информации; совокупность мер по предупреждению компьютерных преступлений.

Цель работы заключается в комплексном уголовно-правовом и криминологическом научном исследовании состояния, тенденций, характерных черт преступлений в сфере компьютерной информации в Российской Федерации.

Задачи исследования:

1. Провести анализ правовых норм, которые устанавливают уголовную ответственность за правонарушения в области компьютерной информации.

2. Рассмотреть сложности квалификации таких правонарушений и проблемы привлечения к уголовной ответственности.

3. Изучить специфику и трудности, возникающие при выявлении и расследовании преступлений, связанных с компьютерной информацией.

В работе используются следующие методы исследования:

1. Историко-правовой — для изучения истории компьютерных преступлений и развития уголовной ответственности;

2. Формально-логический — для подробного анализа уголовно-правовых и организационно-технических мер предотвращения несанкционированного доступа к компьютерной информации;

3. Статистический — для сбора и анализа статистических данных о незаконных действиях в сфере компьютерной информации.

Работа состоит из введения, трёх глав с подпунктами и заключения.

1. ОБЩИЕ ПОЛОЖЕНИЯ УГОЛОВНОГО ЗАКОНОДАТЕЛЬСТВА О ПРЕСТУПЛЕНИЯХ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

1.1 Исторические аспекты, развитие уголовного законодательства РФ за преступления в сфере компьютерной информации

В современном информационном обществе проблема преступности в области информационных технологий приобретает особую актуальность. Тем не менее, важно осознавать, что данная проблематика не является новой для нашего государства. В данном случае целесообразно обратиться к периоду 70–80-х годов XX века, когда началось масштабное внедрение разнообразных технологий, в том числе информационных. Научно-техническая революция XX века кардинально изменила взгляд человечества на мир вокруг нас[1].

Были созданы такие средства связи, как телеграф, телефон, радио, кино, телевидение и компьютер. Это произошло благодаря значительным научным и технологическим достижениям. Эти инновации не только способствовали развитию общества, но и предоставили новые возможности для преступного мира, который начал активно использовать их в своих целях.

Сегодня компьютерные технологии проникли во все сферы человеческой деятельности. Это создаёт новые вызовы и угрозы для безопасности. Киберпреступность становится всё более сложной и масштабной, используя уязвимости цифровых систем для нанесения ущерба как отдельным людям, так и целым организациям. Поэтому развитие законодательства, регулирующего общественные отношения в сфере высоких технологий, становится особенно важным.

[1] Трофимова, А. Ю. История развития уголовного законодательства в части регламентации оснований ответственности за преступления в сфере компьютерной информации / А. Ю. Трофимова. — Текст : непосредственный // Молодой ученый. — 2021. — № 53 (395). — С. 128-129. — URL: https://moluch.ru/archive/395/87551/

В 70-е годы XX века произошёл скачок в развитии информационных технологий, что, к сожалению, способствовало появлению новых способов использования их в преступных целях. Это стало возможным благодаря распространению компактных компьютерных систем среди широкого круга пользователей.

С развитием интернета и увеличением числа его пользователей, возникла острая необходимость в разработке и внедрении систем защиты информации, направленных на ограничение доступа к сети. Однако, как показывает практика, эти меры не только не уменьшили количество киберпреступлений, а наоборот способствовали их увеличению.

Этот парадокс объясняется возникновением новой профессиональной ниши специалистов по информационной безопасности, которые, стремясь преодолеть защитные механизмы, разрабатывают всё более изощрённые методы взлома.

В начале 90-х годов XX века, когда информационные технологии активно развивались, группа экспертов Интерпола попыталась создать единую классификацию таких преступлений. Эта работа в итоге нашла отражение в «Будапештской конвенции Совета Европы 2001 года».

Конвенция о преступности в сфере компьютерной информации включает в себя следующие главы и разделы:

Глава I - Использование терминов;

Глава II - Меры, которые следует принять на национальном уровне;

Глава II. Раздел 1 - Материальное уголовное право;

Глава II. Раздел 2 - Процессуальное законодательство;

Глава III - Международное сотрудничество;

Глава III. Раздел 1 - Общие принципы международного сотрудничества;

Глава III. Раздел 2 - Общие принципы взаимной помощи;

Глава III. Раздел 3 - Конкретные положения;

Глава IV - Заключительные положения[2].

Страны G7, осознавая значимость и масштабность проблемы, продолжают работать над созданием единого подхода к решению данного вопроса. В условиях, когда компьютерные преступления приобретают транснациональный характер, необходимость унификации уголовного законодательства становится особенно острой.

Компьютерная преступность затронула в своё время и Советский Союз, и впоследствии Россию.

В 1979 году в Вильнюсе было зафиксировано первое преступление в бывшем СССР, связанное с использованием ЭВМ. Ущерб от этого хищения составил 78 584 рубля. Что касается России, то первые преступления с применением компьютерной техники на территории РСФСР были зафиксированы в 1991 году. Тогда во Внешэкономбанке СССР были украдены 125,5 тысяч долларов США[3].

В то время отечественный законодатель впервые занялся разработкой правовых норм, касающихся уголовного права в области использования и распространения информационных технологий. Конечно же речь идёт о проекте Закона РСФСР «Об ответственности за правонарушения при работе с информацией», который был создан в 1991 году. Этот документ предусматривал введение дисциплинарной, гражданско-правовой, административной и уголовной ответственности за соответствующие нарушения.

В 1992 году в Российской Федерации был принят Закон о правовой охране программ для электронно-вычислительных машин и баз данных. Этот документ стал важным шагом в развитии законодательства, регулирующего вопросы использования и защиты компьютерной информации.

[2] Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). URL: https://base.garant.ru/4089723/

[3] Бессонов С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. URL: https://cyberleninka.ru/article/n/istoriya-i-zarubezhnyy-opyt-pravovoy-reglamentatsii-kompyuternoy-prestupnosti/

Например, этот закон содержал следующие статьи[4]:

«Программа для ЭВМ - это объективная форма представления совокупности данных и команд, предназначенных для функционирования электронных вычислительных машин (ЭВМ) и других компьютерных устройств с целью получения определённого результата. Под программой для ЭВМ подразумеваются также подготовительные материалы, полученные в ходе её разработки, и порождаемые ею аудиовизуальные отображения», - Часть 1, Статья 1.

«Использование программы для ЭВМ или базы данных третьими лицами (пользователями) осуществляется на основании договора с правообладателем, за исключением случаев, указанных в статье 16 настоящего Закона», - Часть 1, Статья 14.

«Выпуск под своим именем чужой программы для ЭВМ или базы данных либо незаконное воспроизведение или распространение таких произведений влечёт за собой уголовную ответственность в соответствии с законом», - Статья 20.

В 1994 году был разработан и введён в действие Гражданский кодекс РФ, содержащий ряд положений, касающихся компьютерной информации. Эти положения стали основой для дальнейшего развития законодательства в данной области[5].

Наконец, в 1995 году был принят Федеральный закон «Об информации, информатизации и защите информации», который установил правовые основы для создания, использования и защиты информационных ресурсов в Российской Федерации. Содержал следующие статьи[6]:

«Информатизация - организационный социально - экономический и научно - технический процесс создания оптимальных условий для

[4] Закон РФ "О правовой охране программ для электронных вычислительных машин и баз данных" от 23.09.1992 N 3523-1 (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_1007/

[5] Китайкина Оксана Олеговна РОССИЙСКОЕ ЗАКОНОДАТЕЛЬСТВО ОБ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: ИСТОРИЯ И СОВРЕМЕННОСТЬ // Научный формат. 2020. №7 (10). URL: https://cyberleninka.ru/article/n/rossiyskoe-zakonodatelstvo-ob-ugolovnoy-otvetstvennosti-za-prestupleniya-v-sfere-kompyuternoy-informatsii-istoriya-i-sovremennost/

[6] Федеральный закон "Об информации, информатизации и защите информации" от 20.02.1995 N 24-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_5887/

удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов», - Статья 2.

«Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах)», - Статья 2.

«Контроль за соблюдением требований к защите информации и эксплуатацией специальных программно - технических средств защиты, а также обеспечение организационных мер защиты информационных систем, обрабатывающих информацию с ограниченным доступом в негосударственных структурах, осуществляются органами государственной власти. Контроль осуществляется в порядке, определяемом Правительством Российской Федерации», - Статья 21.

«Защита прав субъектов в сфере формирования информационных ресурсов, пользования информационными ресурсами, разработки, производства и применения информационных систем, технологий и средств их обеспечения осуществляется в целях предупреждения правонарушений, пресечения неправомерных действий, восстановления нарушенных прав и возмещения причинённого ущерба», - Статья 23.

В 1996 году был завершён процесс формирования законодательства, итогом которого стало принятие Уголовного кодекса Российской Федерации[7]. В нём, помимо прочего, была выделена отдельная глава, устанавливающая уголовную ответственность за преступления, совершённые в сфере компьютерной информации. Речь идёт про Главу 28 УК РФ «Преступления в сфере компьютерной информации»[8].

[7] Федеральный закон "О введении в действие Уголовного кодекса Российской Федерации" от 13.06.1996 N 64-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_10701/

[8] УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/

В настоящий момент вопрос о формировании эффективных международных норм, направленных на борьбу с киберпреступлениями, приобретает особую актуальность. Однако, несмотря на растущую потребность в таком регулировании, на сегодняшний день не существует единого нормативного акта, который был бы принят и одобрен на уровне ООН. Более того, анализ последних тенденций показывает, что создание подобного регулирования представляется крайне сложной задачей, поскольку страны Совета Европы активно поддерживают Будапештскую конвенцию 2001 года, которая является единственным международным документом в области уголовного преследования за киберпреступления. Это приводит к тому, что они блокируют любые законодательные инициативы других стран, включая Россию, стремящуюся разработать более эффективные механизмы противодействия киберпреступности.

1.2 Уголовная ответственность за преступления в сфере компьютерной информации по законодательству РФ

Уголовный кодекс Российской Федерации содержит ряд статей, направленных на предотвращение преступлений, связанных с неправомерным доступом к охраняемой законом компьютерной информации. Это такие статьи как: «УК РФ Статья 272. Неправомерный доступ к компьютерной информации», «УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ», «УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», «УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», «УК РФ Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории

Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования»[9].

УК РФ Статья 272. Неправомерный доступ к компьютерной информации, - «Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации».

Чтобы действие было классифицировано как преступление по определённой статье, должны выполняться три обязательных условия:

1. Неправомерность доступа к информации;

2. Специальный правовой режим информации, которая охраняется законом;

3. Последствия, наступившие в результате такого доступа.

Информация, для которой законодательством установлен особый порядок защиты, считается охраняемой законом. К такой информации относятся государственная, служебная и коммерческая тайна, а также персональные данные пользователей.

Если для защиты информации применяются специальные средства, то лицо, не имеющее соответствующих полномочий, не может получить доступ к ней без согласия владельца или его законного представителя.

«Каждый имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Ограничение этого права допускается только на основании судебного решения», - Часть 2, Статьи 23 Конституции Российской Федерации[10].

Исходя из этого следует, что любые попытки нарушить тайну переписки или других видов коммуникации должны быть санкционированы судом. Эта норма является нормой прямого действия и обязательна для

[9] УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/

[10] "Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/

исполнения всеми участниками правовых отношений. Информация, содержащая тайну переписки, находится под особой правовой защитой, так как она охраняется основным законом страны.

«Неправомерный доступ к компьютерной информации – это незаконное либо не разрешённое собственником или иным её законным владельцем использование возможности получения компьютерной информации»[11].

«Неправомерным доступом к компьютерной информации является получение или использование такой информации без согласия обладателя информации лицом, не наделенным необходимыми для этого полномочиями, либо в нарушение установленного нормативными правовыми актами порядка независимо от формы такого доступа. Путём проникновения к источнику хранения информации в компьютерном устройстве, принадлежащем другому лицу, непосредственно либо путём удалённого доступа», - Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N 37[12].

Неправомерный доступ может осуществляться как с целью получения выгоды для себя, так и для нанесения ущерба владельцу информации или другим лицам. Он может привести к утечке конфиденциальной информации, нарушению работы информационных систем и другим негативным последствиям.

Доступ к информации означает получение к ней доступа с помощью компьютерных технологий, что позволяет выполнять различные действия с данными: копировать, изменять, блокировать или удалять их.

Чтобы привлечь лицо к уголовной ответственности за неправомерный доступ к компьютерной информации, необходимо установить факт наступления одного из определённых последствий: уничтожение

[11] Официальный сайт Министерства внутренних дел Российской Федерации // Ответственность за преступления в сфере компьютерной информации. URL: https://34.xn--b1aew.xn--p1ai/document/44685304/

[12] Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N 37 “О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет". URL: https://www.garant.ru/products/ipo/prime/doc/405863329/

информации, блокировка информации, модификация информации или копирование информации.

1. Уничтожение информации — это процесс, при котором информацию или её часть делают непригодной для использования. При этом не имеет значение возможность её восстановления. Это может быть удаление файла, форматирование диска или физическое уничтожение носителя информации.

2. Блокировка информации — это оказание влияния на компьютерные данные или устройства таким образом, что становится невозможным выполнение необходимых операций над этими данными в полном объёме или в нужном режиме в течение определённого периода времени или постоянно. Это может быть вызвано вирусной атакой, сбоем в работе программного обеспечения или физическим повреждением оборудования.

3. Модификация информации — это изменение компьютерной информации или её параметров. Закон разрешает законную модификацию программ и баз данных лицам, имеющим право на эту информацию, в следующих случаях: исправление ошибок; внесение изменений в программы и базы данных для их корректной работы на оборудовании пользователя; декомпиляция программы для частного использования с целью обеспечения взаимодействия с другими программами.

Закон разрешает законную модификацию программ и баз данных лицам, имеющим право на эту информацию, в следующих случаях: исправление ошибок; внесение изменений в программы и базы данных для их корректной работы на оборудовании пользователя; декомпиляция программы для частного использования с целью обеспечения взаимодействия с другими программами.

4. Копирование информации — это процесс создания копии данных на другом носителе. Он включает в себя перенос информации на отдельный носитель без изменения первоначального содержания. Это может быть

сделано с помощью различных устройств и технологий, таких как принтеры, сканеры, USB-накопители и облачные хранилища[13].

Важно отметить, что привлечение к уголовной ответственности возможно только в случае, если действия лица были неправомерными и повлекли за собой одно из указанных последствий. Если же действия были совершены в рамках законных прав и обязанностей, то они не могут быть квалифицированы как преступление.

Статья 272 УК РФ предусматривает следующие виды наказаний за совершённые преступления, - «Наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок»[14].

УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ, - «Создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации».

В данной статье говорится о преступлениях, заключающихся в создании, распространении или использовании компьютерных программ или другой компьютерной информации, которые специально предназначены для несанкционированного удаления, блокировки, изменения, копирования информации или обхода механизмов защиты информации.

[13] Генеральная прокуратура Российской Федерации // Об уголовной ответственности за неправомерный доступ к охраняемой законом компьютерной информации. URL: https://epp.genproc.gov.ru/web/proc_21/activity/legal-education/explain?item=71718675/

[14] УК РФ Статья 272. Неправомерный доступ к компьютерной информации. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/5c337673c261a026c476d578035ce68a0ae86da0/

Необходимо отметить, что эти противоправные деяния ставят под угрозу общественный порядок и безопасность, а также взаимоотношения в социуме, касающиеся легального и надёжного применения информации.

«В законе не закреплено понятие «вредоносные компьютерные программы», но чаще всего к ним относят программы или переносные коды, направленные на хищение информации и подрыв функциональности программного обеспечения»[15].

К вредоносным компьютерным программам относятся различные виды программного обеспечения, такие как компьютерные вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации и многие другие. Эти программы могут нанести серьёзный ущерб компьютерным системам и сетям, похищая конфиденциальную информацию, нарушая работу программного обеспечения и делая системы уязвимыми для дальнейших атак.

Например, знаменитая российская антивирусная компания «Лаборатория Касперского» [16] выделяет наиболее распространённые виды вредоносных компьютерных программ:

1. «Вирусы. Компьютерные вирусы получили своё название из-за способности быстро распространяться и поражать множество файлов на компьютере. Они могут перейти на другие устройства, если заражённые файлы отправить по электронной почте или перенести на физических носителях, таких как USB-накопители или, ранее, дискеты. Компьютерные вирусы очень активно развиваются и адаптируются к новым технологиям и методам защиты. Представляют собой серьёзную угрозу для пользователей компьютеров и информационных систем, поэтому важно принимать меры для защиты от них. Например, стоит переодически обновлять свою

[15] Кшнякина Анастасия Евгеньевна АКТУАЛЬНЫЕ ПРОБЛЕМЫ ПРИМЕНЕНИЯ СТ.273 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ // E-Scio. 2022. №7 (70). URL: https://cyberleninka.ru/article/n/aktualnye-problemy-primeneniya-st-273-ugolovnogo-kodeksa-rossiyskoy-federatsii/

[16] Официальный сайт АО «Лаборатория Касперского». URL: https://www.kaspersky.ru/

операционную систему, использовать антивирусные программы со свежими базами данных, использовать лицензионное программное обеспечение».

2. «Черви. В отличие от тех же самых вирусов, распространение которых требует определённых действий от пользователя, черви могут самостоятельно заражать один компьютер, а затем через сеть распространяться на другие устройства без участия человека. Используя уязвимости в сетевых сервисах, черви могут массово рассылать свои копии и заражать новые системы. Многие черви потребляют компьютерные ресурсы, что снижает производительность устройства, а большинство из них содержат вредоносные компоненты, предназначенные для кражи или удаления файлов».

3. «Рекламное программное обеспечение. Рекламные программы (Adware) — это одни из самых распространённых видов вредоносного ПО. Они предназначены для автоматической демонстрации рекламы на компьютере пользователя. Некоторые рекламные программы относительно безопасны, в то время как другие используют инструменты отслеживания для сбора информации о пользователе. Эти данные затем используются для показа целевой рекламы.. Также относительно недавно стало известно о новом типе рекламного ПО, способном отключать антивирусную защиту на компьютере».

4. «Шпионское программное обеспечение. Программы-шпионы представляют собой серьёзную угрозу для безопасности пользователей компьютеров и других устройств. Предназначены для сбора конфиденциальной информации о действиях пользователя и его устройстве без его ведома или согласия. Такие программы могут выполнять различные функции, например, регистрировать нажатия клавиш на клавиатуре, отслеживать посещённые сайты, собирать регистрационные данные, изменять параметры защиты на компьютере или блокировать сетевые соединения. Собранная информация затем передаётся третьим лицам,

обычно киберпреступникам, которые могут использовать её для различных целей, например, для кражи личных данных, мошенничества или шантажа».

5. «Программы-вымогатели. Данные вредоносные программы проникают в систему, шифруют важные файлы и документы, а затем требуют выкуп за их расшифровку. Если жертва отказывается платить, данные могут быть безвозвратно утеряны. Существуют разные типы программ-вымогателей. Одни блокируют доступ к устройству, другие шифруют только определённые файлы, третьи угрожают опубликовать личные данные пользователя. Такие программы распространяются разными способами: через уязвимости в операционной системе, через заражённые сайты и вложения в электронных письмах».

6. «Боты. Это программы, которые созданы для автоматического выполнения определённых задач. Они могут быть использованы как во благо, так и во вред. Если бот попадает в компьютер, он может заставить устройство выполнять различные команды без разрешения или ведома пользователя. Хакеры могут заражать несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть. С её помощью они могут удалённо управлять взломанными устройствами и использовать их для кражи личных данных, слежки за жертвой, распространения спама».

7. «Руткиты. Руткиты представляют собой программы, которые позволяют получить удалённый доступ к компьютеру и управлять им. Они используются IT-специалистами для диагностики и устранения сетевых проблем на расстоянии. Однако в руках злоумышленников руткиты могут стать инструментом мошенничества. Проникнув в компьютер, они дают киберпреступникам возможность контролировать его, похищать личные данные пользователя или устанавливать другие вредоносные программы. Руткиты умеют качественно маскировать своё присутствие в системе, чтобы оставаться незамеченными как можно дольше».

8. «Троянские программы. Данный тип программ маскируются под безобидные файлы или приложения. Когда пользователь скачивает и

устанавливает такой файл, программа начинает вносить изменения в систему и совершать вредоносные действия без ведома и согласия владельца компьютера. Эти программы могут выполнять разные задачи в зависимости от целей злоумышленника. Например, они могут использоваться для кражи личных данных, рассылки спама, установки другого вредоносного ПО или получения полного контроля над компьютером жертвы».

9. «Баги. Ошибки в программном коде, называемые багами, не являются разновидностью вредоносных программ, а представляют собой недочёты, допущенные разработчиком. Они могут привести к серьёзным проблемам, таким как зависание, сбой или снижение скорости работы компьютера. Баги в системе безопасности предоставляют злоумышленникам лёгкий способ обойти защиту и заразить устройство».

Поскольку компьютерные технологии постоянно развиваются, невозможно составить полный список вредоносных программ.

Поэтому при рассмотрении уголовных дел по данной статье, необходимо проводить экспертизу, чтобы объективно оценить каждую компьютерную программу и определить, является ли она вредоносной.

Преступление может быть совершено только путём действия, которое заключается в разработке вредоносного программного обеспечения, его использовании или распространении.

Статья 273 УК РФ предусматривает следующие виды наказаний за совершённые преступления, - «Наказываются ограничением свободы на срок до четырёх лет, либо принудительными работами на срок до четырёх лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осуждённого за период до восемнадцати месяцев»[17].

УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, - «Нарушение правил эксплуатации средств

[17] УК РФ Статья 273. Создание, использование и распространение вредоносных компьютерных программ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/a4d58c1af8677d94b4fc8987c71b131f10476a76/

хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлёкшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб».

Преступление, о котором идёт речь, нацелено на общественные отношения, связанные с защитой информации в компьютерных системах[18].

Эта норма является общей и чётко указывает на необходимость соблюдения законов, положений, инструкций и правил, которые регулируют работу с информационно-телекоммуникационными сетями и конечным оборудованием в организациях и ведомствах.

Сегодня существует множество официальных правил, которые определяют, как обеспечить безопасность при использовании оборудования для хранения, обработки и передачи данных, а также информационно-телекоммуникационные сетей. Кроме того, существуют индивидуальные требования владельцев по использованию этих средств.

В научных работах высказываются обоснованные точки зрения учёных касательно проблемы привлечения к уголовной ответственности за несоблюдение так называемых «ненормативных» правил. Это вполне логично, поскольку существует множество технических документов на компьютерное оборудование и правил использования различных программ, имеющих рекомендательный характер.

Наилучшим вариантом в данной ситуации считается введение чёткого свода правил работы со средствами хранения, обработки и передачи компьютерной информации, а также с информационно-телекоммуникационными сетями. За нарушение которых будут наступать негативные последствия. Предлагается ввести уголовную ответственность в

[18] Кондратюков Сергей Сергеевич, Лупырь Максим Валерьевич К ВОПРОСУ ОБ ОБЪЕКТЕ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТАТЬЕЙ 274 УГОЛОВНОГО КОДЕКСА РОССИЙСКОЙ ФЕДЕРАЦИИ // Вестник Университета «Кластер». 2022. №4 (4). URL: https://cyberleninka.ru/article/n/k-voprosu-ob-obekte-prestupleniya-predusmotrennogo-statiey-274-ugolovnogo-kodeksa-rossiyskoy-federatsii/

соответствии со статьёй 274 Уголовного кодекса Российской Федерации. Однако такое нововведение не позволит в полной мере решить данную проблему, поскольку разработать и объединить в одном документе все правила использования средств хранения, обработки и передачи компьютерных данных и информационно-телекоммуникационные сетей во всех системах представляется крайне сложной задачей. Даже если попытаться сделать это сейчас, законодателю всё равно придётся неоднократно вносить изменения в эти правила в будущем.

Это связано с тем, что технологии развиваются очень быстро, появляются новые средства хранения, обработки и передачи информации, а также новые способы их использования. Поэтому создать документ, который изначально будет содержать все необходимые правила и будет актуален в течение длительного времени, практически невозможно.

Кроме того, необходимо учитывать, что правила использования информационных систем могут различаться в зависимости от конкретной ситуации. Например, правила использования информационных технологий в государственных органах могут отличаться от правил использования этих же технологий в коммерческих организациях.

В государственных службах и ведомствах вопрос защиты информации частично решён. Например, в системе МВД России предусмотрен комплекс мероприятий по защите информации, которая содержит сведения, составляющие государственную тайну, и сведения конфиденциального характера.

Порядком эксплуатации специального программного обеспечения федеральной информационной системы Госавтоинспекции определяются правила доступа администраторов, пользователей и операторов к информационной системе ведомства.

Статья 274 УК РФ предусматривает следующие виды наказаний за совершённые преступления, - «Наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осуждённого

за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок»[19].

УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Для того чтобы создать надёжную систему критической информационной инфраструктуры (КИИ), в своё время были приняты соответствующие меры.

Одной из таких мер стало принятие Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187-ФЗ[20].

«Критическая информационная инфраструктура - объекты критической информационной инфраструктуры, а также сети электросвязи, используемые для организации взаимодействия таких объектов». - Часть 6, Статьи 2 ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Использование объектов критической информационной инфраструктуры (КИИ) охватывает широкий спектр областей[21]:

1. Медицина и здравоохранение;
2. Наука и техника;
3. Транспорт;
4. Связь;
5. Финансы и экономика;
6. Атомная энергетика;
7. Оборотная промышленность;

[19] УК РФ Статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/b5a4306016ca24a588367791e004fe4b14b0b6c9/

[20] Федеральный закон "О безопасности критической информационной инфраструктуры Российской Федерации" от 26.07.2017 N 187-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_220885/

[21] Горелик Владимир Юдаевич, Безус Михаил Юрьевич О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. №9. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/

8. Ракетостроение;

9. Горнодобывающая отрасль;

10. Металлургия;

11. Химическое производство.

Важность объектов критической информационной инфраструктуры (КИИ) обусловлена тем, что сбой в их работе может иметь серьёзные последствия.

В случае успешной кибератаки на объекты КИИ может произойти катастрофа в общественной, экономической или финансовой сфере. Чтобы предотвратить подобные преступления, был принят Федеральный закон от 26 июля 2017 г. № 194-ФЗ. Данный закон дополняет статью 274.1 УК РФ.

В постановлении Пленума Верховного Суда Российской Федерации от 15 декабря 2022 г. № 37 «О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершённых с использованием электронных или информационно-телекоммуникационных сетей, включая сеть „Интернет“» обращается внимание судов на то, что преступления, предусмотренные статьёй 274 Уголовного кодекса Российской Федерации, признаются оконченными, «когда указанные в части 1 этой статьи деяния повлекли наступление одного или нескольких общественно опасных последствий в виде уничтожения, блокирования, модификации либо копирования охраняемой законом компьютерной информации, а также в виде причинения крупного ущерба»[22].

В документе отмечается, что последствия несанкционированного доступа к охраняемой законом компьютерной информации или использования вредоносных программ должны быть напрямую связаны с этими действиями.

[22] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет". URL: https://www.consultant.ru/document/cons_doc_LAW_434573/

Также в документе указано, что применение вредоносных программ для незаконного воздействия на критическую информационную инфраструктуру России полностью соответствует части 2 статьи 274.1 Уголовного кодекса Российской Федерации.

В статье 274.1 Уголовного кодекса Российской Федерации предусмотрены три отдельных состава преступления, которые являются специальными по отношению к преступлениям, описанным в статьях 272–274 УК РФ.

Первый состав касается создания, распространения и использования компьютерных программ или другой компьютерной информации, специально предназначенных для незаконного воздействия на КИИ России. Это включает уничтожение, блокировку, модификацию, копирование информации, которая в ней содержится, или нейтрализацию средств защиты этой информации.

Второй состав связан с незаконным доступом к охраняемой компьютерной информации, которая содержится в КИИ России. Такой доступ может осуществляться с использованием компьютерных программ или другой компьютерной информации, специально предназначенных для незаконного воздействия на эту инфраструктуру, или других вредоносных программ. Если такой доступ повлёк за собой вред КИИ России, то это является специальным составом по отношению к преступлению, предусмотренному статьёй 272 УК РФ.

Если правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, которая содержится в критической информационной инфраструктуре Российской Федерации, или же информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, были нарушены, что привело к причинению вреда критической информационной инфраструктуре Российской Федерации, это считается специальным

составом преступления, предусмотренного статьёй 274 Уголовного кодекса Российской Федерации.

В соответствии с частью 1 статьи 274.1 Уголовного кодекса Российской Федерации, уголовная ответственность наступает за разработку, передачу и применение специального компьютерного программного обеспечения и данных, направленных на несанкционированное воздействие на объекты критической информационной инфраструктуры (КИИ).

Использование программ и информации, предназначенных для противоправных действий, таких как незаконное уничтожение, блокировка, изменение или копирование информации, а также принудительное отключение средств защиты компьютерных данных, ставит вопрос о квалификации существующего программного обеспечения.

Несмотря на то, что законодательство не проводит различий между программами, предназначенными для воздействия на КИИ, и другими видами вредоносного программного обеспечения, анализ судебной практики показывает, что злоумышленники могут использовать различные инструменты, изначально разработанные для других целей, для нанесения ущерба объектам критической информационной инфраструктуры.

Преступление считается совершённым с момента создания, передачи или использования таких программ, независимо от последствий.

В соответствии с частью 2 статьи 274.1 Уголовного кодекса РФ, противозаконный доступ к защищённой компьютерной информации, которая хранится в критически важной информационной инфраструктуре Российской Федерации, в том числе с применением компьютерных программ или другой компьютерной информации, специально созданных для незаконного воздействия на эту инфраструктуру, или любых других вредоносных программ, если это привело к ущербу для критически важной информационной инфраструктуры РФ, является преступлением. Это указывает на то, что данное правонарушение имеет материальный состав.

В соответствии с частью 3 статьи 274.1 Уголовного кодекса Российской Федерации, нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, а также информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления и сетей электросвязи, которые относятся к критической информационной инфраструктуре Российской Федерации, влечёт за собой уголовную ответственность. Это касается и нарушения правил доступа к указанной информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления и сетям электросвязи.

Если такие нарушения привели к причинению вреда критической информационной инфраструктуре Российской Федерации, то за это предусмотрена уголовная ответственность.

Важно отметить, что конкретные правила эксплуатации и доступа к объектам критической информационной инфраструктуры не прописаны напрямую в Федеральном законе «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 года № 187. Вместо этого используются общие требования по созданию безопасных условий для значимых объектов критической информационной инфраструктуры.

В Уголовном кодексе Российской Федерации предусмотрены особые обстоятельства, которые усугубляют ответственность за неправомерное воздействие на критическую информационную инфраструктуру. Это включает действия, совершённые группой лиц по предварительной договорённости или организованной группой, а также лицами, использующими своё служебное положение. Также к таким обстоятельствам относится наступление серьёзных последствий.

Как упоминалось ранее, результаты могут проявиться в любой отрасли, так как объекты КИИ классифицируются по категориям, важным для

определённой сферы деятельности. Последствия могут быть катастрофическими.

КИИ связывает различные секторы национальной инфраструктуры, поэтому повреждение одного звена влияет на работу остальных. Это может привести к серьёзному ущербу для объектов жизнеобеспечения и оборонной отрасли, а также к гибели людей.

В качестве примера можно привести ситуацию, когда из-за сбоя в системе электроснабжения происходит отключение электроэнергии в крупном городе. Это может привести к остановке работы предприятий, нарушению работы транспорта, а также к другим негативным последствиям.

Кроме того, сбой в системе управления транспортом может привести к массовым ДТП, а сбой в системе водоснабжения — к отключению воды в жилых домах и на предприятиях.

Статья 274.1 предусматривает следующие виды наказаний за совершённые преступления:

Часть 1 Статьи 274.1, - «Наказываются принудительными работами на срок до пяти лет с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до трёх лет».

Часть 2 Статьи 274.1, - «Наказывается принудительными работами на срок до пяти лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до трёх лет и с ограничением свободы на срок до двух лет или без такового либо лишением свободы на срок от двух до шести лет со штрафом в размере от пятисот тысяч до одного миллиона рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до трёх лет».

Часть 3 Статьи 274.1, - «Наказывается принудительными работами на срок до пяти лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет или без такового либо лишением свободы на срок до шести лет с лишением права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет или без такового»[23].

УК РФ Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования.

В соответствии со статьёй 274.2 Уголовного кодекса РФ, если должностные лица или индивидуальные предприниматели, которые уже были привлечены к административной ответственности за нарушение правил установки, эксплуатации или модернизации технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования интернета и сетей связи общего пользования, повторно нарушат эти правила, то они могут быть привлечены к уголовной ответственности. «Наказывается штрафом в размере от семисот тысяч до полутора миллионов рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо принудительными работами на срок до трёх лет, либо лишением свободы на тот же срок».

Должностные лица и индивидуальные предприниматели, которые нарушили требования к пропуску трафика через технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования и уже были подвергнуты административному наказанию за это, также могут быть привлечены к

[23] УК РФ Статья 274.1. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/34672bc8c82c4b6f4b7c8cd4e77a9f414fed6cb1/

уголовной ответственности. «Наказывается штрафом в размере от семисот тысяч до полутора миллионов рублей или в размере заработной платы или иного дохода осуждённого за период от одного года до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо принудительными работами на срок до трёх лет, либо лишением свободы на тот же срок»[24].

[24] УК РФ Статья 274.2. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/56d15b1ae0a6eb1d6405f9ffe9aa48e21351f445/

2. ОБЩИЕ ВОПРОСЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

2.1 Объективные признаки компьютерных преступлений

В современном мире, где информационные технологии играют ключевую роль в жизни общества, вопрос о сущности компьютерных преступлений становится особенно актуальным. Компьютерные преступления, являясь разновидностью преступлений информационного характера, требуют детального исследования их объективной стороны.

Введение уголовной ответственности за преступления, связанные с неправомерными действиями с компьютерной информацией, является необходимой мерой, обусловленной рядом факторов[25].

Для полного понимания сущности компьютерных преступлений как преступлений в сфере информации необходимо тщательно исследовать их объективную сторону.

Одним из таких преступлений является неправомерный доступ к компьютерной информации. Он влечёт за собой уголовную ответственность в случаях несанкционированного доступа к информации, защищённой законом, что приводит к её уничтожению, блокированию, модификации или копированию, а также к нарушению работы ЭВМ, системы ЭВМ или их сети. Важно установить причинно-следственную связь между этими действиями и наступившими последствиями.

Состав преступления, связанного с неправомерным доступом к компьютерной информации, имеет сложную и неоднозначную объективную сторону.

Одним из действий, которые запрещены законом и составляют объективную сторону преступления, является неправомерный доступ к

[25] Яковенко Ирина Александровна ОБЪЕКТИВНЫЕ ПРИЗНАКИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ КАК РАЗНОВИДНОСТИ ПРЕСТУПЛЕНИЙ ИНФОРМАЦИОННОГО ХАРАКТЕРА // E-Scio. 2021. №2 (53). URL: https://cyberleninka.ru/article/n/obektivnye-priznaki-kompyuternyh-prestupleniy-kak-raznovidnosti-prestupleniy-informatsionnogo-haraktera/

компьютерной информации. В научных работах неправомерный доступ к информации описывается как несанкционированное использование данных, не разрешённое собственником или законным владельцем. Доступ к компьютерной информации подразумевает любую возможность взаимодействия с источником данных, позволяющую манипулировать этими данными, например, копировать, изменять, блокировать или удалять их.

В рамках данного исследования также рассматривается разработка, применение и распространение вредоносного программного обеспечения, что является ещё одним видом преступлений в сфере информационных технологий. Согласно статье 273 Уголовного кодекса Российской Федерации, объективная сторона этого преступления включает в себя несколько возможных действий:

1. Создание компьютерных программ или иной компьютерной информации, которая заведомо способна привести к несанкционированному уничтожению, блокированию, модификации, копированию компьютерной информации или нейтрализации средств защиты компьютерной информации;

2. Использование таких программ или информации;

3. Распространение подобных программ или информации.

Для квалификации деяния по данной статье достаточно совершения хотя бы одного из перечисленных действий.

С точки зрения объективных признаков, ключевым понятием является «программа». В контексте компьютерных технологий, программа — это алгоритм решения задачи, предназначенный для исполнения на электронных устройствах.

Чтобы программа была признана использованной в контексте объективной стороны преступления, описанного в статье 273 УК РФ, необходимо, чтобы с ней непосредственно работали и применяли её согласно назначению.

Одним из признаков объективной стороны состава преступления является распространение вредоносных компьютерных программ. Это

преступное деяние включает в себя предоставление доступа к таким программам любым посторонним лицам любыми способами, в том числе через продажу, аренду, бесплатную рассылку по электронной почте.

Следующим рассматриваемым составом преступления является нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей по статье 274 УК РФ. Объективную сторону этого преступления составляют действия, нарушающие правила эксплуатации указанных средств и сетей, а также правила доступа к ним. Эти действия должны привести к уничтожению, блокированию, модификации или копированию компьютерной информации и причинить крупный ущерб. Законодатель описывает этот состав преступления как материальный, то есть преступление считается совершённым не с момента совершения запрещённого действия, а с момента наступления последствий в виде крупного ущерба.

В отличие от других составов компьютерных преступлений, которые были рассмотрели ранее, данное преступное деяние характеризуется тем, что оно может быть совершено как путём действия, так и путём бездействия со стороны виновного лица. Учёные в целом согласны с таким подходом к определению преступного деяния.

Чтобы полностью и детально проанализировать признаки объективной стороны преступления, описанного в статье 274 УК РФ, нужно обратиться к специальным нормативным документам. Диспозиция этой статьи носит бланкетный характер, то есть её содержание раскрывается через ссылки на другие нормативные акты. К таким документам относятся законы, подзаконные акты, технические стандарты, регламенты, санитарно-эпидемиологические правила и нормативы, рекомендации государственных органов, а также локальные правовые акты.

Чтобы квалифицировать деяние как преступление, правоохранительным органам нужно не только сослаться на определённую

правовую норму, но и выявить, в чём заключается правонарушение и как действия обвиняемого нарушают установленный порядок.

Как отмечалось ранее, состав преступления определяется исходя из материальных признаков, что подразумевает не только совершение противоправного действия, но и установление факта возникновения общественно опасных последствий.

В итоге, можно сказать, что выявление объективной стороны компьютерных преступлений представляет собой сложную задачу. В некоторых случаях для этого достаточно установить факт совершения противоправного действия (ст. 272 УК РФ), а в других ситуациях необходимо также доказать наличие определённых преступных последствий (ст. 273, 274, 274.1, 274.2 УК РФ).

2.2. Субъективные признаки компьютерных преступлений

В каждом преступлении есть субъективная сторона, которая характеризуется наличием вины, мотива и цели у лица, совершившего общественно опасное и противоправное деяние.

Это позволяет понять, что происходит с психикой человека, который нарушает закон, а также увидеть связь между мыслями преступника и его действиями. Но если говорить о незаконном доступе к компьютерной информации, то ответственность за такие действия не всегда одинакова.

Преступления в сфере компьютерной информации — это общественно опасные деяния, которые предусмотрены уголовным законодательством и представляют угрозу для информации и информационных ресурсов.

Конфиденциальность информации — это характеристика, которая определяется субъективно и указывает на то, что доступ к определённой информации должен быть ограничен кругом лиц, имеющих соответствующие полномочия. Это свойство обеспечивается способностью системы сохранять эту информацию в секрете от тех, кто не имеет права доступа к ней.

Целостность информации означает, что информация сохраняется в первоначальном виде без изменений. Однако для субъектов важно обеспечить ещё более широкое свойство — достоверность информации, которая включает в себя такие аспекты, как полнота и точность отображения реального положения дел в определённой области.

Доступность информации — это возможность получить нужные данные в любое время, когда это необходимо. Это свойство системы, в которой циркулирует информация, обеспечивающее своевременный и лёгкий доступ к интересующим данным и постоянную готовность автоматизированных служб обрабатывать запросы пользователей.

Следственно, для автоматизированных систем можно рассматривать три основных вида угроз: угроза нарушения конфиденциальности; угроза нарушения целостности; угроза отказа служб.

В уголовном праве субъектом преступления считается человек, который совершил преступное деяние и может быть привлечён к уголовной ответственности за свои действия или бездействие.

В соответствии со статьёй 272 Уголовного кодекса Российской Федерации, существуют две категории лиц, которые могут быть привлечены к ответственности за неправомерный доступ к охраняемой законом компьютерной информации: общий субъект и специальный субъект.

В уголовном праве выделяется общий субъект преступления — это вменяемое физическое лицо, достигшее возраста 16 лет. Также существует специальный субъект преступления, который помимо общих признаков субъекта преступления обладает дополнительными признаками, необходимыми для привлечения его к уголовной ответственности за конкретное совершённое преступление.

Субъект преступления действует с прямым умыслом. Он осознаёт, что создаёт, использует или распространяет вредоносную программу или файл. Всё это противозаконные действия.

Момент вины проявляется либо в стремлении к достижению определённых результатов, либо в сознательном допущении возможности их наступления, либо как минимум в безразличном отношении к возможным последствиям.

В российском законодательстве существует важный принцип, который гласит, что деяние, совершённое по неосторожности, может быть признано преступлением только в том случае, если это прямо указано в соответствующей статье Особенной части Уголовного кодекса.

В Уголовном кодексе РФ есть принцип, согласно которому действие, не предусматривающее возможность совершения по неосторожности, считается умышленным. Это правило зафиксировано во второй части статьи 24 УК РФ.

Этот принцип особенно важен в контексте статьи 272 УК РФ, которая устанавливает ответственность за неправомерный доступ к компьютерной информации. Поскольку в этой статье не упоминается возможность совершения преступления по неосторожности, можно сделать вывод, что неправомерный доступ к охраняемой законом компьютерной информации может быть совершён только умышленно.

Таким образом, можно заключить, что при рассмотрении дел, связанных с неправомерным доступом к компьютерной информации, определение степени осознания лицом противоправности своих действий и его отношения к возможным последствиям этих действий играет ключевую роль в установлении наличия вины и, как следствие, в вынесении справедливого решения.

Согласно законодательству Российской Федерации, каждый человек, достигший шестнадцатилетнего возраста, может быть признан субъектом преступления, предусмотренного частью 1 статьи 272 УК РФ. Однако для привлечения к уголовной ответственности важно, чтобы лицо было признано вменяемым. Если же человек признан невменяемым, он не может быть привлечён к уголовной ответственности в соответствии со статьёй 21 УК РФ.

Также Уголовный кодекс Российской Федерации содержит статью 273, которая устанавливает ответственность за разработку, распространение или использование компьютерных программ, предназначенных для незаконного уничтожения, блокировки, изменения или копирования данных на компьютере. Такие программы обычно представляют собой компьютерные вирусы различных типов: троянские кони, черви, кейлоггеры, руткиты и другие.

Преступление, описанное в части 1 статьи 273 Уголовного кодекса Российской Федерации, совершается с прямым умыслом. Если кто-то использует вредоносную программу для личных целей, например, для удаления собственной информации с компьютера, это не является наказуемым деянием. Преступление может совершить только тот, кто осознаёт свои действия и способен отвечать за них, и кому уже исполнилось 16 лет.

Важно подчеркнуть, что злоумышленники нередко применяют вредоносное ПО для осуществления других преступлений, в частности, для кражи денег у пострадавших. Именно поэтому большинство уголовных дел по статье 273 УК РФ инициируется на основании заявлений от физических или юридических лиц о краже денежных средств с использованием вредоносных программ[26].

Следом за 273 статьёй 273 УК РФ идёт статья 274 УК РФ, которая устанавливает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

В юридической практике часто возникают трудности с определением субъективной стороны преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Это

[26] Волженин Вячеслав Владимирович К вопросу о квалификации, раскрытии и расследовании преступлений, предусмотренных статьей 273 УК РФ // Вестник науки и образования. 2019. №24-2 (78). URL: https://cyberleninka.ru/article/n/k-voprosu-o-kvalifikatsii-raskrytii-i-rassledovanii-prestupleniy-predusmotrennyh-statiey-273-uk-rf/

обусловлено тем, что разные авторы предлагают различные подходы к пониманию субъективной стороны таких преступлений. Некоторые исследователи считают, что субъективная сторона этих преступлений характеризуется только неосторожной формой вины. Они аргументируют свою позицию тем, что нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей обычно происходит из-за невнимательности, небрежности или легкомыслия. Другие авторы полагают, что субъективная сторона этих преступлений может быть как умышленной, так и неосторожной. Они указывают на то, что в некоторых случаях лица, нарушающие правила эксплуатации, могут делать это намеренно, осознавая возможные последствия своих действий. Также существует мнение, что субъективная сторона этих преступлений характеризуется двумя формами вины. Это означает, что в отношении одних последствий лицо действует умышленно, а в отношении других — по неосторожности. Анализируя норму, которая является бланкетной, можно сделать вывод, что лицо, нарушающее правила, осознаёт возможность возникновения негативных последствий, но безосновательно надеется их избежать. Либо не предвидит эти последствия, хотя при должной внимательности и осторожности могло бы их предсказать.

Чтобы вина содержала интеллектуальный момент, необходимо, чтобы нарушитель знал о правилах, которые он нарушает. Это знание подтверждается фактом ознакомления с этими правилами, которое может быть зафиксировано в договоре, инструкции, пользовательском соглашении и других документах.

Согласно статье 274 Уголовного кодекса РФ, субъектом преступления может быть физическое лицо старше 16 лет, которое является вменяемым. Однако существуют разные мнения относительно того, кто может быть субъектом этого преступления. Некоторые исследователи считают, что субъект должен быть специальным, поскольку он может определяться не

только обязанностями, возложенными на лицо инструкциями или договорами, но и фактическим использованием лицом определённых ресурсов и оборудования. Это означает, что субъект определяется его включённостью в специфические общественные отношения[27].

Статья 274.1 УК РФ. С точки зрения субъективной стороны, составы преступлений, предусмотренные частями 1 и 2 статьи 274.1 Уголовного кодекса Российской Федерации, характеризуются наличием вины в форме умысла. Это означает, что лицо, совершающее указанные действия, осознаёт их общественную опасность и предвидит возможность или неизбежность наступления общественно опасных последствий. Деяние, описанное в части 3 статьи 274.1 Уголовного кодекса РФ, может быть совершено как умышленно, так и по неосторожности. Это связано с тем, что сбои в работе автоматизированных систем управления могут произойти как из-за случайных ошибок в системе, так и в результате намеренных действий.

Законодатель не указал мотивы и цели в качестве обязательных или отягчающих обстоятельств ни в одном из составов преступлений, включая квалифицированные. Причины такого решения вызывают вопросы, поскольку аналогичный подход применяется к регулированию некоторых других видов киберпреступлений.

Конечно, посягательства на КИИ РФ могут совершаться по самым разным мотивам. Корыстные не занимают последнее место. Также неоднородными выступают цели преступления. Одни увеличивают степень общественной опасности, а другие - нет.

Направленность общественно опасного деяния и предполагаемый преступником результат имеют ключевое значение. Исследования показывают, что многие киберпреступления направлены на совершение других противоправных действий. Это создаёт цепочку правонарушений, в

[27] Стяжкина Светлана Александровна УГОЛОВНО-ПРАВОВЫЕ ОСОБЕННОСТИ КВАЛИФИКАЦИИ НАРУШЕНИЯ ПРАВИЛ ЭКСПЛУАТАЦИИ СРЕДСТВ ХРАНЕНИЯ, ОБРАБОТКИ ИЛИ ПЕРЕДАЧИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ И ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ (СТАТЬЯ 274 УК РФ) // Вестник Удмуртского университета. Серия «Экономика и право». 2021. №3. URL: https://cyberleninka.ru/article/n/ugolovno-pravovye-osobennosti-kvalifikatsii-narusheniya-pravil-ekspluatatsii-sredstv-hraneniya-obrabotki-ili-peredachi-kompyuternoy/

которой первоначальное компьютерное преступление служит основой для последующих преступлений. Субъектом данного преступления может быть физическое и вменяемое лицо старше 16 лет[28].

Согласно статье 274.2 УК РФ, субъектом преступления в обоих случаях является должностное лицо, которое выполняет управленческие, организационные или хозяйственные функции в коммерческой или другой организации на постоянной, временной или специальной основе, а также индивидуальный предприниматель, ранее привлечённый к административной ответственности за соответствующие нарушения, предусмотренные КоАП РФ.

В статье 274.2 УК РФ прямо не раскрывается субъективная сторона преступления. Однако, учитывая формальную конструкцию составов, можно сделать вывод, что субъективная сторона нарушения специальных правил (ч. 1 ст. 274.2 УК РФ) и нарушения требований к пропуску трафика (ч. 2 ст. 274.2 УК РФ) выражается виной в виде прямого умысла[29].

[28] Мосечкин Илья Николаевич ПРОБЛЕМЫ УГОЛОВНО-ПРАВОВОЙ ОХРАНЫ КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ // Всероссийский криминологический журнал. 2023. №1. URL: https://cyberleninka.ru/article/n/problemy-ugolovno-pravovoy-ohrany-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/

[29] Евгений Александрович Русскевич Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. №3. URL: https://cyberleninka.ru/article/n/narushenie-pravil-tsentralizovannogo-upravleniya-tehnicheskimi-sredstvami-protivodeystviya-ugrozam-informatsionnoy-bezopasnosti/

3. ПРОБЛЕМЫ КВАЛИФИКАЦИИ КОМПЬЮТЕРНЫХ ПРЕСТУПЛЕНИЙ

3.1 Особенности квалификации компьютерных преступлений в зависимости от объективных признаков

Как обозначалось ранее в данной работе для правильного определения общественной опасности совершённого деяния и вынесения соответствующего наказания существуют критерии, обозначающие объект преступления, объективную сторону, субъект и субъективную сторону деяния.

Объективная сторона включает в себя следующие элементы состава преступления:

1. Общественно опасное деяние;
2. Последствия общественно опасного деяния;
3. Связь между деянием и его результатами;
4. Место, время и метод совершения правонарушения.

В соответствии со статьёй 272 Уголовного кодекса РФ, наказание предусмотрено за несанкционированный доступ к данным, хранящимся на компьютере, если это привело к потере данных, их изменению, копированию или созданию препятствий для доступа к ним, а также вызвало сбой в работе компьютерных систем.

Необходимо, чтобы существовала прямая связь между незаконными действиями в отношении защищаемых данных и возникшими в результате этого негативными последствиями. Преступление, описанное в статье 272, считается завершённым после того, как наступают общественно опасные последствия[30].

[30] Симаков С.А. ОБЪЕКТИВНЫЕ И СУБЪЕКТИВНЫЕ ПРИЗНАКИ ПРЕСТУПЛЕНИЯ, ПРЕДУСМОТРЕННОГО СТ. 272 УК РФ // Вестник науки. 2023. №11 (68). URL: https://cyberleninka.ru/article/n/obektivnye-i-subektivnye-priznaki-prestupleniya-predusmotrennogo-st-272-uk-rf/

Общественные отношения, которые связаны с безопасным использованием компьютеров, становятся объектом преступного посягательства.

Преступление может быть совершено с применением специальных технических или программных средств, а также с использованием действующих учётных данных пользователей. Кроме того, преступники могут похищать цифровые носители информации, хотя это и предполагает организацию охраны таких носителей. Предметом преступного посягательства в данном случае является компьютерная информация.

Рассмотрим судебную практику по данной статье. ФИО2 совершила умышленное преступление - неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло блокирование, модификацию, копирование компьютерной информации, при следующих обстоятельствах. В период времени с 00 часов 01 минуты 01 ноября 2022 года до 08 часов 36 минут 02 декабря 2022 года, более точные дата и время не установлены, у ФИО2, находящейся в неустановленном месте на территории г. Новомосковска Тульской области, возник преступный умысел, направленный на неправомерный доступ к охраняемой законом компьютерной информации, а именно к аккаунту «Яндекс ID» Потерпевший №1 – «<адрес>», который повлечёт её модификацию, блокирование и копирование, с целью последующего использования указанной информации в личных целях. С целью реализации своего преступного умысла ФИО2, осознавая противоправность и общественную опасность своих действий, умышленно, неустановленным способом, находясь в указанный период времени в неустановленном месте на территории г. Новомосковска Тульской области, приискала в сети «Интернет» посредством неустановленного Telegram-бота, основанного на платформе интернет-мессенджера «Telegram», сведения об анкетных данных Потерпевший №1, включающих в себя его фамилию, имя, отчество, дату рождения, адрес регистрации и местожительства, абонентский номер телефона №, используемый

Потерпевший №1, адрес его электронной почты <адрес>, дату её регистрации и ранее использованные им пароли. Далее ФИО2, используя заранее подготовленные средства связи и технические средства, позволяющие осуществлять доступ в сеть «Интернет» и подконтрольные ей абонентские номера, умышленно, реализуя свой преступный умысел, из личной заинтересованности, совершила неправомерный доступ к охраняемой законом компьютерной информации, повлёкший её модификацию, блокирование и копирование, с целью последующего использования данной информации в личных целях. Суд приговорил: признать ФИО2 виновной в совершении преступления, предусмотренного ч.1 ст.272 УК РФ[31].

Далее следует статья 273 УК РФ Создание, использование и распространение вредоносных компьютерных программ. Согласно статье 273 УК РФ, объективная сторона преступления заключается в совершении одного или нескольких определённых действий. Разработка и подготовка программ, в том числе путём изменения существующих программ, а также другой компьютерной информации, предназначенной для несанкционированного доступа к данным без согласия их владельца или в нарушение установленных правил по уничтожению, изменению, копированию информации или отключению средств её защиты, является созданием вредоносных программ или иной вредоносной компьютерной информации.

Чтобы квалифицировать действия человека по первой части статьи 273 УК РФ как оконченное преступление, достаточно доказать, что он создал фрагмент кода вредоносной компьютерной программы, который позволяет получить несанкционированный доступ к информации. Если же создание полноценной вредоносной программы не было завершено, действия человека будут расцениваться как создание другой вредоносной компьютерной информации. Важно отметить, что использование программ или информации на собственных или с согласия владельца компьютерных устройствах без

[31] «Судебные и нормативные акты РФ». Приговор № 1-298/2023 от 9 ноября 2023 г. по делу № 1-298/2023. URL: https://sudact.ru/regular/doc/MY7l09LHkBoJ/

намерения незаконно получить доступ к защищённой законом информации и без ущерба для этой информации или её защиты (например, в образовательных целях или для тестирования систем безопасности с законным доступом), а также разработка таких программ для этих целей не считается преступлением[32]. Пример судебной практики. ФИО2 совершил использование и распространение компьютерных программ, заведомо предназначенных для несанкционированного блокирования компьютерной информации и нейтрализации средств защиты компьютерной информации, совершенные из корыстной заинтересованности. Преступление совершено в Валуйском городском округе Белгородской области при таких обстоятельствах. ФИО2 в неустановленное в ходе проведения следствия время, но не позднее 04.03.2021г., приобрёл игровую консоль «Sony PlayStation 3» серии 02-27445988-1442043-CECH-4208C с комплектующими (джойстиком и USB шнурами) для личного использования, после чего у него возник и сформировался прямой преступный умысел, направленный на использование и дальнейшее распространение вредоносных компьютерных программ. В целях реализации своего преступного умысла, ФИО2 в неустановленное в ходе проведения следствия время, но не позднее 04.03.2021 года, будучи собственником игровой консоли «Sony PlayStation 3», являющейся электронно-вычислительной машиной, действуя умышленно, в целях использования компьютерных программ, заведомо предназначенных для несанкционированного блокирования компьютерной информации и нейтрализации средств защиты компьютерной информации, достоверно зная, что правообладателем и владельцем исключительных прав на программное обеспечение указанной игровой консоли является корпорация «Сони Интерэктив Интертейнмент Инк.», в нарушение положений ч. 1 ст. 44 Конституции РФ, гарантирующей охрану интеллектуальной собственности в Российской Федерации, положений Гражданского кодекса РФ,

[32] Генеральная прокуратура Российской Федерации // Уголовная ответственность создание, использование и распространение вредоносных компьютерных программ (прокуратура г. Новомосковска). URL: https://epp.genproc.gov.ru/web/proc_71/activity/legal-education/explain?item=89688271/

лицензионного соглашения пользователя на системное программное обеспечение системы «PlayStation®3», условий использования программ компании «Сони Интерэктив Интертейнмент Инк.» использовал ранее установленные на указанную игровую консоль компьютерные программы: «HEN 3.0.2 RUS», «HEN Toolbox Mod» и «webMAN Mod», которые предназначены для несанкционированного блокирования компьютерной информации и нейтрализации средств защиты компьютерной информации в своих целях вплоть до 01.04.2021 года. Затем у ФИО2 сформировался прямой преступный умысел, направленный на распространение из корыстной заинтересованности игровой консоли Sony PlayStation 3» с установленными на ней компьютерными программами, которые предназначены для несанкционированного блокирования, компьютерной информации и нейтрализации средств защиты компьютерной информации. Реализуя свой прямой умысел, ФИО2, не ранее 04.03.2021 года посредством сети Интернет, через сайт «Авито», указав для связи принадлежащий ему абонентский номер телефона №, подал объявление о продаже игровой консоли «Sony PlayStation 3» за денежные средства в размере 12 000,00 рублей. Суд приговорил: Признать ФИО2 виновным в совершении преступления, предусмотренного ст. 273 ч.2 УК РФ и назначить ему по этой статье наказание в виде ограничения свободы сроком на 6 (шесть) месяцев[33].

Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Суть этого преступления заключается в несоблюдении правил использования устройств для хранения, обработки или передачи данных, а также сетей связи, что привело к потере, изменению или копированию информации и нанесло значительный ущерб. Состав данного преступления, описанный в соответствующей статье, считается завершённым только при условии нанесения значительного ущерба. Важно установить причинно-следственную связь между нарушением правил и нанесённым

[33] «Судебные и нормативные акты РФ». Приговор № 1-100/2021 от 30 июля 2021 г. по делу № 1-100/2021. URL: https://sudact.ru/regular/doc/9U1XWCSz3Vo1/

ущербом. Последствия должны быть прямым результатом нарушения правил эксплуатации, а не программных ошибок или действий, предусмотренных статьями 272 и 273 Уголовного кодекса.

Преступления, связанные с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, отличаются от преступлений, предусмотренных статьёй 272 УК РФ. В случае неправомерного доступа к охраняемой законом компьютерной информации виновный не имеет права её использовать, то есть действует незаконно. При этом состав нарушения правил эксплуатации предполагает, что виновный, в силу своего служебного положения, получает доступ к информации на законных основаниях.

Статья 274.1 УК РФ. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

В рамках части 1 статьи 274.1 Уголовного кодекса РФ, объективная сторона преступления включает в себя три альтернативных действия:

1. Создание;

2. Распространение;

3. Использование компьютерных программ или иной компьютерной информации, специально разработанных для незаконного воздействия на критически важную информационную инфраструктуру Российской Федерации, включая уничтожение, блокировку, модификацию, копирование информации, содержащейся в ней, или нейтрализацию средств защиты этой информации.

Преступление, описанное в части 1 статьи 274.1 УК РФ, считается завершённым с момента совершения любого из перечисленных действий.

Часть 2 статьи 274.1 Уголовного кодекса Российской Федерации предусматривает ответственность за неправомерный доступ к охраняемой компьютерной информации, которая содержится в критической информационной инфраструктуре РФ. Этот доступ может осуществляться с использованием компьютерных программ или иной информации, специально

предназначенной для неправомерного воздействия на критическую информационную инфраструктуру РФ, а также с применением вредоносных программ.

Одним из обязательных условий для квалификации данного деяния как преступления является причинение вреда критической информационной инфраструктуре РФ в результате такого неправомерного доступа к охраняемой компьютерной информации. Это может выражаться в уничтожении, блокировании, модификации или копировании такой информации.

Часть 3 статьи 274.1 Уголовного кодекса РФ предусматривает ответственность за действия, которые нарушают правила использования или правила допуска к объектам критической информационной инфраструктуры РФ. К таким объектам относятся:

1. Средства хранения, обработки охраняемой компьютерной информации;
2. Информационные системы;
3. Информационно-телекоммуникационные сети;
4. Автоматизированные системы управления;
5. Сети электросвязи.

Это преступление считается совершённым, если был причинён вред критической информационной инфраструктуре РФ.

Пример судебной практики. ФИО2 на основании трудового договора № <...>-крд от 03.02.2022 года был принят на работу на должность специалиста офиса Публичного акционерного общества «Вымпел-коммуникации» (далее по тексту ПАО «ВымпелКом») в подразделении офиса обслуживания и продаж с дислокацией в <адрес>. В период работы в его должностные обязанности входило, в том числе: обеспечивать обработку персональных данных субъектов ПДН (физических лиц), с которыми связана работа сотрудника, в том числе сбор, хранение, ввод, использование, изменение и уничтожение обрабатываемых персональных данных, в соответствии с

законодательством и внутренними нормативными документами компании; соблюдать режим защиты и обработки персональных данных, меры безопасности, при всех видах обработки персональных данных, включая сбор, передачу, хранение, использование, уничтожение, и трансграничную передачу в соответствии с законодательством и внутренними нормативными документами компании; обеспечивать конфиденциальность обрабатываемых персональных данных в соответствии с законодательством, внутренними нормативными документами компании; не разглашать информацию ограниченного доступа, в том числе информацию, составляющую коммерческую тайну, которые ему будут доверены или станут известны по работе; не предавать третьим лицам и не раскрывать публичную информацию ограниченного доступа без согласия компании. Согласно приложению к обязательству о неразглашении, а именно перечню сведений ограниченного распространения, составляющую коммерческую тайну компании, к сведениям ограниченного доступа относятся: сведения, касающиеся режима доступа к ресурсам информационной системы компании, а также сведения о персональных данных клиентов компании, образцах их подписей и печатей. 18.01.2023 в период времени с 14 часов 00 минут до 15 часов 00 минут, ФИО2, находясь на своём рабочем месте в офисе по адресу: <адрес>, имея умысел направленный на неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации, с использованием своего служебного положения, осознавая противоправный характер и общественную опасность своих действий, используя служебный компьютер, вошёл в свою учётную запись «ФИО2», при помощи штатных программ «АСРМ Продакшн-Терминал» и «1-С» после чего произвёл перенос абонентского номера № <...> на сим-карту носитель имеющуюся в салоне сотовой связи «Билайн» без участия владельца абонентского номера. Продолжая реализовывать свой преступный умысел предоставил персональные данные абонентского номера № <...> третьему лицу, тем самым полностью реализовав свой преступный умысел. Таким

образом, ФИО2 совершил преступление, предусмотренное ч. 4 ст. 274.1 УК РФ – нарушение правил обработки и передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации, лицом с использованием своего служебного положения. Суд приговорил: ФИО2 признать виновным в совершении преступления, предусмотренного ч.4 ст. 274.1 УК РФ и назначить ему наказание с применением ст. 64 УК РФ в виде лишения свободы на срок 1 (Один) год[34].

Статья 274.2 УК РФ. Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования.

В части 1 статьи 274.2 Уголовного кодекса РФ говорится об ответственности за несоблюдение правил установки, использования и модернизации технических средств, предназначенных для защиты от угроз устойчивому функционированию интернета и сетей связи общего пользования, а также за невыполнение технических требований к установке этих средств или их использованию.

Субъект преступления может действовать активно или пассивно. В частности, он может мешать дистанционному управлению техническими средствами противодействия угрозам со стороны радиочастотной службы, нарушать требования эксплуатационной документации, отключать технические средства от электропитания или блокировать доступ к оборудованию для представителей радиочастотной службы.

Часть 2 статьи 274.2 Уголовного кодекса Российской Федерации предусматривает ответственность за нарушение правил пропуска трафика через технические средства защиты от угроз. Эти правила установлены

[34] «Судебные и нормативные акты РФ». Приговор № 1-168/2023 от 12 октября 2023 г. по делу № 1-168/2023. URL: https://sudact.ru/regular/doc/WorWKo6DbRN8/

приказом Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 26 января 2022 г. № 44.

В обоих составах преступлений используется принцип административной преюдиции. Это означает, что нарушение правил должно быть совершено в то время, когда лицо уже было привлечено к административной ответственности.

3.2 Особенности квалификации компьютерных преступлений в зависимости от субъективных признаков

Субъективная сторона компьютерных преступлений характеризуется прямым или косвенным умыслом.

Прямой умысел выражается в том, что правонарушитель осознает общественно опасный характер своего деяния, предвидит наступление общественно опасных последствий и желает их наступления.

Косвенный умысел заключается в том, что правонарушитель осознает общественно опасный характер своего действия или бездействия, предвидит общественно опасные последствия и сознательно допускает их.

В соответствии со статьёй 272 УК РФ, неправомерный доступ к охраняемой законом компьютерной информации влечёт за собой уголовную ответственность. Вина в совершении данного преступления может быть как умышленной (прямой или косвенный умысел), так и неосторожной. Субъектом преступления может быть любое вменяемое лицо, достигшее 16-летнего возраста.

Однако часть 3 статьи 272 УК РФ предусматривает наличие специального субъекта, который совершил это преступление, используя своё служебное положение. Использование служебного положения в контексте части 3 статьи 272 УК РФ означает возможность доступа к компьютерной информации, которая возникла в результате работы (по трудовому или

гражданско-правовому договору) или влияния по службе на лиц, имеющих такой доступ.

В этом случае субъектом преступления может быть не только должностное лицо, но и любой человек, который на законных основаниях использует компьютерную информацию и средства её обработки. Это могут быть программисты, сотрудники, вводящие информацию в память компьютера, другие пользователи, а также администраторы баз данных, инженеры, ремонтники, специалисты по эксплуатации электронно-вычислительной техники и другие.

Таким образом, субъектом преступления по части 3 статьи 272 УК РФ может быть широкий круг лиц, которые имеют доступ к компьютерной информации в силу своих профессиональных обязанностей или влияния по службе. Важно отметить, что для привлечения к уголовной ответственности необходимо установить наличие умысла или неосторожности в действиях лица, а также факт наступления последствий, предусмотренных частью 1 статьи 272 УК РФ (уничтожение, блокирование, модификация либо копирование компьютерной информации).

Преступление, предусмотренное статьёй 272 УК РФ, является умышленным и может быть совершенно только с умыслом прямым или косвенным, то есть, когда лицо осознавало общественную опасность своих действий, предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления, либо не желало, но сознательно допускало наступление этих последствий либо относилось к ним безразлично. Действия, формально попадающие под диспозицию статьи 272 УК РФ, но совершённые по легкомыслию или небрежности, не являются уголовно-наказуемыми.

Возраст, с достижением которого виновное лицо может быть привлечено к уголовной ответственности, установлен законодателем в 16 лет. Федеральным законом от 13.06.2023 № 214-ФЗ предусмотрена конфискация имущества есть принудительное безвозмездное изъятие и обращение в

собственность государства на основании обвинительного приговора денег, ценностей и иного имущества, полученных в результате совершения преступлений, предусмотренных частями 2–4 статьи 272 УК РФ.

Статья 273 УК РФ направлена на предотвращение и пресечение действий, связанных с созданием, использованием и распространением вредоносных компьютерных программ. Эти действия могут нанести значительный ущерб как отдельным лицам, так и организациям, а также обществу в целом.

Часть 1 статьи 273 УК РФ предусматривает наказание за создание, распространение или использование компьютерных программ или информации, которые предназначены для несанкционированного уничтожения, блокирования, модификации или копирования компьютерной информации или нейтрализации средств её защиты.

Состав преступления характеризуется виной в форме прямого умысла. Это означает, что виновный должен осознавать, что создаваемые или используемые им программы заведомо приведут к общественно опасным последствиям, указанным в законе. Мотив и цель не влияют на квалификацию преступления.

Субъект преступления — общий: вменяемое лицо, достигшее 16 лет.

Часть 3 статьи 273 УК РФ предусматривает квалифицирующий признак рассматриваемого состава преступления — наступление тяжких последствий или создание угрозы их наступления. Если наступили тяжкие последствия, то состав преступления является материальным, то есть деяние считается оконченным с момента наступления общественно опасных последствий. Если же создана угроза их наступления, то состав является усечённым.

Тяжесть последствий определяется с учётом всех обстоятельств дела: причинение особо крупного материального ущерба, серьёзное нарушение деятельности предприятий и организаций, наступление аварий и катастроф, причинение тяжкого и средней тяжести вреда здоровью людей или смерти,

уничтожение, блокирование, модификация или копирование привилегированной информации особой ценности, реальность созданной угрозы и другие обстоятельства.

Субъективная сторона указанного квалифицированного состава преступления характеризуется двумя формами вины: умыслом по отношению к самому деянию и неосторожностью по отношению к последствиям. Если преступник умышленно относился к наступлению тяжких последствий или созданию угрозы их наступления, то его действия подлежат дополнительной квалификации по совокупности преступлений, предусмотренных соответствующими статьями УК РФ, в зависимости от качественной и количественной оценки наступивших тяжких последствий.

Таким образом, статья 273 УК РФ играет важную роль в обеспечении безопасности компьютерной информации и средств её защиты, устанавливая строгие меры ответственности за создание, использование и распространение вредоносных компьютерных программ.

Статья 274 УК РФ регулирует ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Это может включать в себя как умышленное, так и неосторожное нарушение этих правил.

Умышленное нарушение означает, что лицо сознательно нарушает установленные правила, например, используя служебный компьютер для личных целей, зная, что это запрещено внутренними правилами организации.

Неосторожное нарушение происходит, когда лицо не предвидит возможных негативных последствий своих действий, хотя должно было и могло их предвидеть. Примером может служить ситуация, когда программист устанавливает программу на компьютер без предварительной проверки на наличие вирусов, что приводит к сбою в работе системы и потере важных данных.

Часть 2 статьи 274 УК РФ предусматривает ответственность за действия, которые привели к тяжким последствиям или создали угрозу их наступления. Тяжкие последствия могут включать в себя значительный материальный ущерб, серьёзное нарушение деятельности предприятия или организации, а также причинение вреда здоровью людей.

Важно отметить, что ответственность за нарушение правил эксплуатации и доступа может варьироваться в зависимости от конкретных обстоятельств каждого случая. В некоторых случаях может быть применена административная ответственность, а в других — уголовная.

Для предотвращения нарушений правил эксплуатации и доступа необходимо соблюдать все установленные правила и инструкции, а также проводить регулярные проверки и обучение персонала. Это поможет снизить риск возникновения нарушений и обеспечить безопасность информационных систем.

Кроме того, важно регулярно обновлять программное обеспечение и антивирусные программы, чтобы минимизировать риски заражения вирусами и другими вредоносными программами. Также следует ограничивать доступ к важным данным и системам только тем сотрудникам, которым это действительно необходимо для выполнения своих обязанностей.

В случае возникновения подозрений на нарушение правил эксплуатации или доступа, необходимо провести внутреннее расследование и принять соответствующие меры для предотвращения подобных ситуаций в будущем.

Субъективная сторона преступлений, предусмотренных частями 1 и 2 статьи 274.1 Уголовного кодекса Российской Федерации, характеризуется умышленной виной. Это означает, что лицо, совершающее эти действия, осознаёт их опасность для общества и предвидит возможность или неизбежность наступления общественно опасных последствий.

Преступление, описанное в части 3 статьи 274.1 Уголовного кодекса РФ, может быть совершено как умышленно, так и по неосторожности. Это

связано с тем, что сбои в работе автоматизированных систем управления могут произойти как из-за случайных ошибок в системе, так и в результате намеренных действий.

Умышленное совершение преступления предполагает, что лицо сознательно нарушает правила эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к ней, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, предвидя возможность или неизбежность наступления общественно опасных последствий.

Неосторожное совершение преступления подразумевает, что лицо не предвидело возможности наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия.

Таким образом, субъективная сторона преступлений, предусмотренных статьёй 274.1 УК РФ, имеет важное значение для квалификации деяния и определения степени ответственности виновного лица.

Умысел может проявляться в различных формах: прямой или косвенный. Прямой умысел характеризуется тем, что лицо осознаёт общественную опасность своих действий (бездействия), предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления. Косвенный умысел отличается от прямого тем, что лицо осознаёт общественную опасность своих действий (бездействия), предвидит возможность наступления общественно опасных последствий, не желает, но сознательно допускает эти последствия либо относится к ним безразлично.

Неосторожность также может проявляться в двух формах: легкомыслие и небрежность. Легкомыслие характеризуется тем, что лицо предвидит возможность наступления общественно опасных последствий своих действий (бездействия), но без достаточных оснований самонадеянно рассчитывает на предотвращение этих последствий. Небрежность проявляется в том, что лицо не предвидит возможности наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия.

Важно отметить, что субъективная сторона преступлений, предусмотренных статьёй 274.1 УК РФ, требует тщательного анализа всех обстоятельств дела, чтобы правильно квалифицировать деяние и определить степень ответственности виновного лица.

В соответствии со статьёй 274.2 Уголовного кодекса Российской Федерации, нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, а также нарушение требований к пропуску трафика через эти технические средства, влечёт за собой уголовную ответственность.

Субъективная сторона преступления, то есть психическое отношение лица к совершаемому им общественно опасному деянию, в данном случае характеризуется умышленной формой вины. Это означает, что лицо, совершившее преступление, осознавало общественную опасность своих действий (бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления, либо не желало, но сознательно допускало эти последствия, либо относилось к ним безразлично.

Умышленная форма вины предполагает, что лицо, совершившее преступление, действовало с прямым или косвенным умыслом. В первом случае лицо осознавало общественную опасность своих действий

(бездействия), предвидело возможность или неизбежность наступления общественно опасных последствий и желало их наступления. Во втором случае лицо осознавало общественную опасность своих действий (бездействия), предвидело возможность наступления общественно опасных последствий, не желало, но сознательно допускало эти последствия, либо относилось к ним безразлично.

Таким образом, субъективная сторона нарушения специальных правил, предусмотренных частью 1 статьи 274.2 УК РФ, и нарушения требований к пропуску трафика, указанных в части 2 статьи 274.2 УК РФ, характеризуется умышленной формой вины, что предполагает осознание лицом общественной опасности своих действий (бездействия), предвидение возможности или неизбежности наступления общественно опасных последствий и желание их наступления, либо сознательное допущение этих последствий, либо безразличное отношение к ним.

Такое понимание субъективной стороны преступления позволяет более точно квалифицировать действия лиц, нарушающих правила и требования, предусмотренные статьёй 274.2 УК РФ, и назначать справедливое наказание в соответствии с тяжестью совершённого деяния.

ЗАКЛЮЧЕНИЕ

В современном мире информация играет ключевую роль во всех сферах деятельности, и компьютерная информация становится всё более значимой. Это требует повышения уровня её защиты с помощью технических, организационных и правовых мер. Одной из причин роста компьютерной преступности является активное внедрение информационных технологий в работу предприятий, учреждений и организаций. Насыщение компьютерной техникой, программным обеспечением и базами данных создаёт новые возможности для злоумышленников. Недостаток комплексных мер противодействия и высокая латентность преступлений в сфере компьютерной информации затрудняют борьбу с этим видом общественно опасных деяний. Для снижения латентности необходимо международное и внутреннее сотрудничество между государством и правоохранительными органами. Также важно проводить разъяснительные работы о необходимости защиты законных интересов в сфере информационных технологий и повышать уровень технического оснащения и квалификацию сотрудников правоохранительных органов.

Для эффективной борьбы с компьютерной преступностью необходимо принять ряд организационных мер:

1. Увеличить штатную численность подразделений, специализирующихся на выявлении и раскрытии преступлений в сфере компьютерной информации.
2. Подбирать в эти подразделения специалистов с глубокими знаниями в области информационно-телекоммуникационных технологий и постоянно совершенствовать их квалификацию.
3. Непрерывно совершенствовать научные методики, программные средства и технические устройства для получения и закрепления доказательств совершения компьютерного преступления в ответ на появление новых механизмов и средств передачи данных.

4. Развивать международное сотрудничество в области обмена опытом и технологиями противодействия компьютерной преступности.

5. Укреплять международное и внутреннее законодательство в области защиты информации и борьбы с киберпреступностью.

6. Повышать осведомлённость населения о рисках, связанных с компьютерной преступностью, и способах защиты от неё.

7. Стимулировать исследования в области информационной безопасности и разработки новых технологий защиты информации.

8. Обеспечивать финансирование и поддержку специализированных образовательных программ и курсов по информационной безопасности.

9. Создавать и поддерживать специализированные центры и лаборатории по исследованию и разработке технологий защиты информации. Разрабатывать и внедрять стандарты и рекомендации по обеспечению информационной безопасности в различных областях деятельности.

Эти меры помогут повысить уровень защиты компьютерной информации, снизить риски компьютерной преступности и обеспечить более эффективную борьбу с ней.

Однако стоит отметить, что борьба с компьютерной преступностью требует комплексного подхода, включающего не только технические и организационные меры, но и правовые аспекты. Необходимо укреплять международное и внутреннее законодательство в области защиты информации и борьбы с киберпреступностью, а также повышать осведомлённость населения о рисках, связанных с компьютерной преступностью, и способах защиты от неё.

Также важно стимулировать исследования в области информационной безопасности и разработки новых технологий защиты информации. Это позволит создать более эффективные методы и средства защиты компьютерной информации, что в свою очередь снизит риски компьютерной преступности.

Кроме того, необходимо обеспечивать финансирование и поддержку специализированных образовательных программ и курсов по информационной безопасности. Это позволит подготовить квалифицированные кадры, способные эффективно бороться с компьютерной преступностью и обеспечивать защиту компьютерной информации.

Таким образом, комплексный подход к борьбе с компьютерной преступностью, включающий технические, организационные, правовые и образовательные аспекты, позволит повысить уровень защиты компьютерной информации и снизить риски компьютерной преступности.

СПИСОК ИСПОЛЬЗУЕМЫХ ИСТОЧНИКОВ И ЛИТЕРАТУРЫ

Нормативно-правовые акты

1. Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 г.). URL: https://base.garant.ru/4089723/

2. Конституция Российской Федерации" (принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020). URL: https://www.consultant.ru/document/cons_doc_LAW_28399/2573feee1caecac37c442734e00215bbf1c85248/

3. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 29.05.2024) (с изм. и доп., вступ. в силу с 10.06.2024). URL: https://www.consultant.ru/document/cons_doc_LAW_10699/

4. УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ. URL: https://www.consultant.ru/document/cons_doc_LAW_10699/4398865e2a04f4d3cd99e389c6c5d62e684676f1/

5. Об информации, информатизации и защите информации. Федеральный закон: от 20.02.1995 N 24-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_5887/

6. О введении в действие Уголовного кодекса Российской Федерации. Федеральный закон: от 13.06.1996 N 64-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_10701/

7. О безопасности критической информационной инфраструктуры Российской Федерации. Федеральный закон: от 26.07.2017 N 187-ФЗ (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_220885/

8. О правовой охране программ для электронных вычислительных машин и баз данных. Закон РФ: от 23.09.1992 N 3523-1 (последняя редакция). URL: https://www.consultant.ru/document/cons_doc_LAW_1007/

9. Постановление Пленума Верховного Суда РФ от 15 декабря 2022 г. N 37 О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет". URL: https://www.garant.ru/products/ipo/prime/doc/405863329/

Судебная практика

10. «Судебные и нормативные акты РФ». Приговор № 1-100/2021 от 30 июля 2021 г. по делу № 1-100/2021. URL: https://sudact.ru/regular/doc/9U1XWCSz3Vo1/

11. «Судебные и нормативные акты РФ». Приговор № 1-168/2023 от 12 октября 2023 г. по делу № 1-168/2023. URL: https://sudact.ru/regular/doc/WorWKo6DbRN8/

12. «Судебные и нормативные акты РФ». Приговор № 1-298/2023 от 9 ноября 2023 г. по делу № 1-298/2023. URL: https://sudact.ru/regular/doc/MY7l09LHkBoJ/

Литература

13. Бессонов, С.А. История и зарубежный опыт правовой регламентации компьютерной преступности // Территория науки. 2013. №2. URL: https://cyberleninka.ru/article/n/istoriya-i-zarubezhnyy-opyt-pravovoy-reglamentatsii-kompyuternoy-prestupnosti/

14. Волженин, В.В. К вопросу о квалификации, раскрытии и расследовании преступлений, предусмотренных статьей 273 УК РФ //

Вестник науки и образования. 2019. №24-2 (78). URL: https://cyberleninka.ru/article/n/k-voprosu-o-kvalifikatsii-raskrytii-i-rassledovanii-prestupleniy-predusmotrennyh-statiey-273-uk-rf/

15. Горелик, В.Ю., Безус М.Ю. О безопасности критической информационной инфраструктуры Российской Федерации // StudNet. 2020. №9. URL: https://cyberleninka.ru/article/n/o-bezopasnosti-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/

16. Китайкина О.О. Российское законодательство об уголовной ответственности за преступления в сфере компьютерной информации: история и современность // Научный формат. 2020. №7 (10). URL: https://cyberleninka.ru/article/n/rossiyskoe-zakonodatelstvo-ob-ugolovnoy-otvetstvennosti-za-prestupleniya-v-sfere-kompyuternoy-informatsii-istoriya-i-sovremennost/

17. Кондратюков С.С, Лупырь М.В. К вопросу об объекте преступления, предусмотренного статьёй 274 Уголовного кодекса Российской Федерации // Вестник Университета «Кластер». 2022. №4 (4). URL: https://cyberleninka.ru/article/n/k-voprosu-ob-obekte-prestupleniya-predusmotrennogo-statiey-274-ugolovnogo-kodeksa-rossiyskoy-federatsii/

18. Кшнякина А.Е. Актуальные проблемы применения ст.273 Уголовного кодекса Российской Федерации // E-Scio. 2022. №7 (70). URL: https://cyberleninka.ru/article/n/aktualnye-problemy-primeneniya-st-273-ugolovnogo-kodeksa-rossiyskoy-federatsii/

19. Мосечкин И.Н. Проблемы уголовно-правовой охраны критической информационной инфраструктуры Российской Федерации // Всероссийский криминологический журнал. 2023. №1. URL: https://cyberleninka.ru/article/n/problemy-ugolovno-pravovoy-ohrany-kriticheskoy-informatsionnoy-infrastruktury-rossiyskoy-federatsii/

20. Русскевич Е.А. Нарушение правил централизованного управления техническими средствами противодействия угрозам информационной безопасности // Journal of Digital Technologies and Law. 2023. №3. URL:

https://cyberleninka.ru/article/n/narushenie-pravil-tsentralizovannogo-upravleniya-tehnicheskimi-sredstvami-protivodeystviya-ugrozam-informatsionnoy-bezopasnosti/

21. Симаков С.А. Объективные и субъективные признаки преступления, предусмотренного ст. 272 УК РФ // Вестник науки. 2023. №11 (68). URL: https://cyberleninka.ru/article/n/obektivnye-i-subektivnye-priznaki-prestupleniya-predusmotrennogo-st-272-uk-rf/

22. Стяжкина С.А. Уголовно-правовые особенности квалификации нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (СТАТЬЯ 274 УК РФ) // Вестник Удмуртского университета. Серия «Экономика и право». 2021. №3. URL: https://cyberleninka.ru/article/n/ugolovno-pravovye-osobennosti-kvalifikatsii-narusheniya-pravil-ekspluatatsii-sredstv-hraneniya-obrabotki-ili-peredachi-kompyuternoy/

23. Трофимова, А. Ю. История развития уголовного законодательства в части регламентации оснований ответственности за преступления в сфере компьютерной информации / А. Ю. Трофимова. — Текст : непосредственный // Молодой ученый. — 2021. — № 53 (395). — С. 128-129. — URL: https://moluch.ru/archive/395/87551/

24. Яковенко И.А. Объективные признаки компьютерных преступлений как разновидности преступлений информационного характера // E-Scio. 2021. №2 (53). URL: https://cyberleninka.ru/article/n/obektivnye-priznaki-kompyuternyh-prestupleniy-kak-raznovidnosti-prestupleniy-informatsionnogo-haraktera/

Электронные источники

25. Генеральная прокуратура Российской Федерации // Об уголовной ответственности за неправомерный доступ к охраняемой законом

компьютерной информации. URL: https://epp.genproc.gov.ru/web/proc_21/activity/legal-education/explain?item=71718675/

26. Генеральная прокуратура Российской Федерации // Уголовная ответственность создание, использование и распространение вредоносных компьютерных программ (прокуратура г. Новомосковска). URL: https://epp.genproc.gov.ru/web/proc_71/activity/legal-education/explain?item=89688271/

27. Официальный сайт Министерства внутренних дел Российской Федерации // Ответственность за преступления в сфере компьютерной информации. URL: https://34.xn--b1aew.xn--p1ai/document/44685304/