Министерство внутренних дел Российской Федерации

Федеральное государственное казенное образовательное учреждение высшего образования «Казанский юридический институт

Министерства внутренних дел Российской Федерации»

Кафедра уголовного права

ДИПЛОМНАЯ РАБОТА

на тему: Преступления в сфере компьютерной информации: юридический анализ и проблемы квалификации

Выполнил: Самсонов Илья Константинович

(фамилия, имя, отчество)

Правовое обеспечение национальной безопасности

(специальность, год набора, № группы)

2020 год набора, 101 уч. гр.

Руководитель:

кандидат юридических наук, доцент, доцент кафедры

(ученая степень, ученое звание, должность)

уголовного права Амирова Диляра Кафилевна

(фамилия, имя, отчество)

Рецензент:

Начальник отдела полиции № 9 «Сафиуллина»

(должность, специальное звание)

УМВД России по г. Казани, подполковник полиции

Зарипов Альберт Ильшатович

(фамилия, имя, отчество)

Дата защиты: «__»_____2025 Оценка _____

Казань 2025

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Актуальность темы дипломной работы. На современном этапе развития научно-технического прогресса уделяется много внимания совершенствованию компьютерных технологий, которые получают все более широкое распространение в жизни общества. Это непосредственно связано с возрастающей ролью информации, важность которой для нормального существования современного общества не вызывает сомнений.

В нашем мире высоких технологий неслучайно появилось выражение: «Кто владеет информацией, тот владеет миром». Наш XXI век смело можно назвать веком высоких технологий и стремительной цифровизации. Информация стала играть одну из ключевых ролей повседневной жизни, а современное общество напрямую зависит от получаемых, обрабатываемых и передаваемых данных. По этой причине данные сами по себе стали весьма ценными. И чем больше «цена такого товара», тем выше «цена» их утери**.** Таким образом, у человечества возник объект, доселе привычный, но поменявший свою форму, который нуждается в защите путем закрепления соответствующих норм в законодательстве страны и введение санкций за их нарушение.

Ценностью обладает не только информация, несущая в себе какие-либо данные и сведения о личной жизни человека, но и также критически важных информационных объектов государства. На государственном уровне компьютерная информация приобрела свое колоссальное значение. Большинство услуг, предоставляемых государством, происходит, в первую очередь, в онлайн формате. С каждым годом просматривается тенденция по возрастанию количества преступлений, которые, так или иначе, затрагивают информационные потоки в нашем государстве. Информация становится не только ключевым объектом, но и особым ресурсом.

С каждым годом преступные умы и их объединения находят все новые и новые способы получения информации, её искажения, уничтожения в своих целях. Иными словами, возник особый вид совершаемых преступлений –

киберпреступность[1]. Это цельная, хороша развитая система преступлений, включающая в себя обширный комплекс противоправных деяний, как внутри, так вне государственного уровня, совершаемых с использованием различных цифровых устройств и сетей.

Кроме того, в последнее время участились атаки на государственные структуры из враждебных по отношению к Российской Федерации государств. Происходит рассылка, запугивание, попытка уничтожения критической инфраструктуры российских Интернет-ресурсов, провайдеров, операторов связи, официальных сайтов государственных учреждений, силовых ведомств и т.д. Добрались также и до обычных граждан.

Быстрое развитие информационно-коммуникационных технологий сопровождается повышением вероятности возникновения угроз безопасности граждан, общества и государства. Расширяется использование информационно-коммуникационных технологий для вмешательства во внутренние дела государств, подрыва их суверенитета и нарушения территориальной целостности, что представляет угрозу международному миру и безопасности. В связи с этим, целью обеспечения информационной безопасности, как указывается в Указе Президента РФ от 02.07.2021 N 400 «О Стратегии национальной безопасности Российской Федерации» (далее по тексту – Стратегия) является укрепление суверенитета Российской Федерации в информационном пространстве[2]. Одной из задач, направленных на достижение этой цели, является - создание условий для эффективного предупреждения, выявления и пресечения преступлений и иных

[1] Прим. автора: В действующем законодательстве Российской Федерации отсутствует определение термина «киберпреступность». В рамках данной выпускной квалификационной работы под киберпреступностью мы понимаем совокупность всех преступлений, в рамках которой используются либо атакуются компьютер, компьютерная сеть или отдельно взятое сетевое устройство.

[2] О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 N 400 // СПС «Консультант плюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения 10.05.2025).

правонарушений, совершаемых с использованием информационно-коммуникационных технологий (п. 57 Стратегии).

С каждым годом фиксируется рост преступлений, совершаемы в сфере высоких технологий. Так, по данным МВД России в 2024 году 40% преступлений были совершены с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 13,1 % больше, чем в 2023 году, в том числе тяжких и особо тяжких составов – на 7,8 %. В значительной степени этот фактор повлиял на рост в 2024 году общего числа тяжких и особо тяжких преступлений на 4,8 %[1] (См. рисунок 1). Значительный рост преступлений отмечается в 2022 году (522065) и в 2024 году составил уже 765365. Из них, значительная доля приходится на преступления против собственности: мошенничества (ст. ст. 159, 159^3, 159^6 Уголовного Кодекса Российской Федерации[2] (далее по тексту – УК РФ)) – 380344 преступлений, кражи (ст. 158 УК РФ) - 105937 преступлений, незаконные производство, сбыт или пересылка наркотических средств, психотропных веществ, а также незаконные сбыт или пересылка растений, содержащих наркотические средства или психотропные вещества ст. 228^1 УК РФ (94645 преступлений).

Несмотря на то, что киберпреступления давно вышли за рамки главы 28 Уголовного кодекса Российской Федерации (далее по тексту – УК РФ), и охватывают собой иные объекты уголовно-правовых отношений, тем не менее на практике возникают трудности, связанные с их квалификацией.

Практика применения уголовного законодательства свидетельствует о том, что возникающие в борьбе с компьютерными преступлениями проблемы обусловлены несовершенством уголовно-правовых норм, противоречивостью

---

[1]Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года // МВД РФ. Официальный сайт – URL: https://мвд.рф/reports/item/60248328/ (дата обращения 01.03.2025).

[2] Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 01.03.2025).

их толкования, отсутствием научно-методических рекомендаций и официальных руководящих разъяснений по квалификации этих деяний. Учитывая стремительное развитие компьютерных технологий, от законодателя требуется быстрое реагирования и своевременное совершенствование уголовного закона.

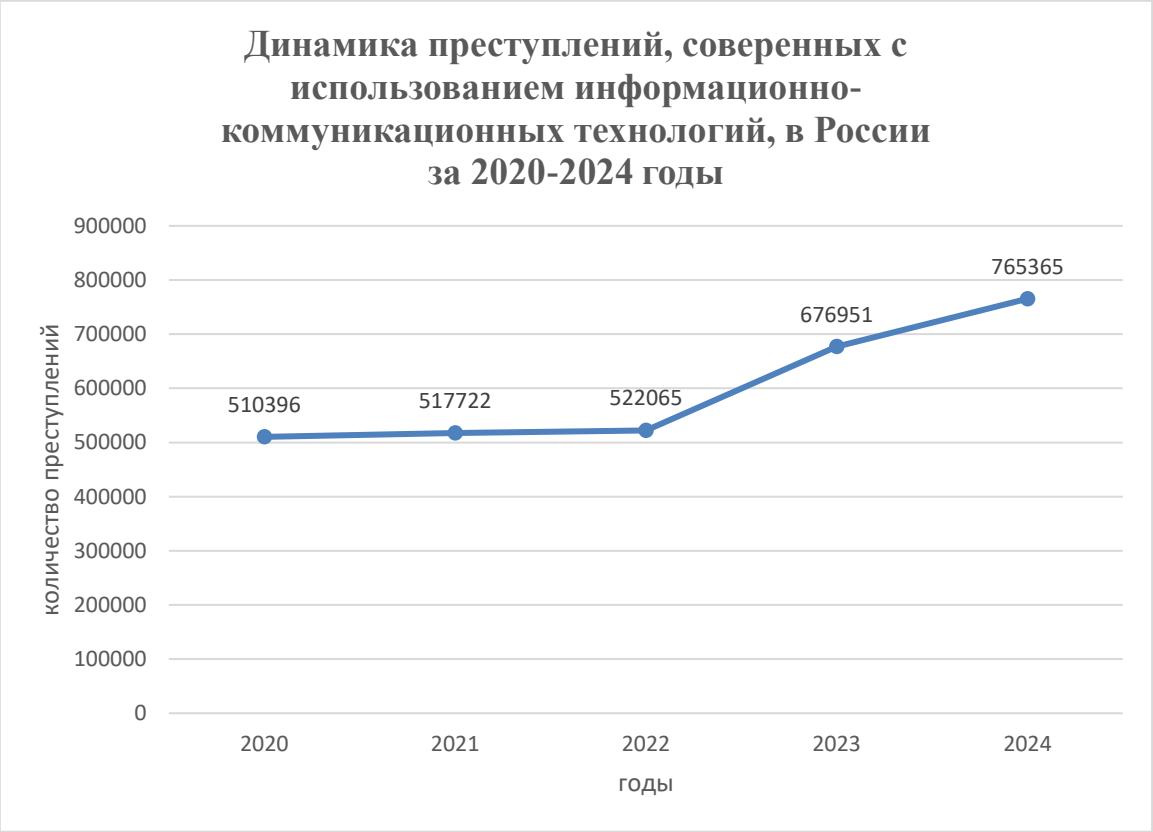

Рисунок 1. Динамика преступлений, совершенных с использованием информационно-коммуникационных технологий, в Российской Федерации за 2020-2025 годы

Практика применения уголовного законодательства свидетельствует о том, что возникающие в борьбе с компьютерными преступлениями проблемы обусловлены несовершенством уголовно-правовых норм, противоречивостью их толкования, отсутствием научно-методических рекомендаций и официальных руководящих разъяснений по квалификации этих деяний. Учитывая стремительное развитие компьютерных технологий, от законодателя требуется быстрое реагирования и своевременное

совершенствование уголовного закона. Актуальной задачей для государства становится совершенствование форм и методов противодействия этим посягательствам. Вот почему теоретическое осмысление вопросов уголовной ответственности за совершение компьютерных преступлений, а также вопросов квалификации является необходимым и целесообразным для теории и практики уголовного права.

Степень научной разработанности темы выпускной квалификационной работы. Следует отметить достаточно высокую степень научной разработанности отдельных вопросов рассматриваемой темы об уголовной ответственности за преступления в сфере компьютерной информации. Так, свои исследования проблему уголовно-правового противодействия данному виду преступности посвятили такие ученые, как: Р.М. Айсанов, И.Р. Бегишев, И.А. Клепицкий, Ю.И. Ляпунов, И.В. Никифоров, А.Э. Побегайло, В.Г. Степанов-Ягинянц, Мозжерина Е. С., Квятковский К. С., Е. А. Русскевич, С. С. Витвицкая, Е. В. Никульченкова и др.

Диссертационные исследования по данной теме проводились М. С. Гаджиевой, Д. В. Добровольским, К.Н. Евдокимовым, А. А. Жмыховой, Т. М. Лопатиной, и др.

Немаловажный вклад в развитие темы внесли зарубежные ученые, такие как: Д. Айков, В. А. Голубев, И. В. Ерень, П. Джонстон, А. Кемрадж, М. Кратц, Д. Лэнс, К. Сейгер, Б. Х. Толеубекова, Ф. Файте, У. Фонсторх, В. В. Хилюта и др.

Указанные работы заложили научные основы уголовно-правового противодействия компьютерной преступности в Российской Федерации. Между тем проблемные вопросы, связанные с квалификацией компьютерной преступности в Российской Федерации в условиях ее трансформации в высокотехнологическую, технотронную преступность; выявления лиц, их совершивших; определения предмета, объекта, определения размера ущерба остались по-прежнему неразрешенными как на научно-теоретическом и законодательном, так и практическом уровнях.

Принятие УК РФ в 1996 году поставило ряд проблем перед теоретиками уголовно-правовой науки: определить объект преступлений в сфере компьютерной информации, сформулировать их понятие и систему; установить критерии выделения близких по содержанию видов преступных посягательств, отграничение от смежных составов преступлений; решить проблему квалификации и ответственности и наказания за них. Кроме того, в теории отечественного уголовного права исследованы и разрешены не все аспекты проблемы ответственности за преступления в сфере компьютерной информации.

Вот почему преступления в сфере компьютерной информации как объект научного исследования требует дальнейшего теоретического изучения и тщательного анализа, в том числе разработки эффективной системы уголовно-правовых мер для противодействия данному негативному социальному явлению. В связи с этим тема выпускной квалификационной работы является актуальной, её исследование в рамках данной работы целесообразным и своевременным для теории и практики уголовного права.

Целью работы является – получение новых знаний об особенностях уголовной ответственности за совершение преступлений в сфере компьютерной информации, разработка и обоснование рекомендаций по совершенствованию действующего уголовного законодательства в рассматриваемой сфере и практики его применения.

Исходя из поставленной цели, выделяются следующие **задачи**:

1. Уяснение понятия, сущности и системы преступлений в сфере компьютерной информации;

2. Изучение статистических данных о количестве и динамике преступлений, совершенных в сфере компьютерной информации;

3. Исследование истории развития уголовного законодательства в РФ и зарубежных странах за преступления в сфере компьютерной информации, а также современной правовой базы зарубежных стран, предусматривающей ответственность за эти преступления;

4. Проведение юридического анализа составов преступлений в сфере компьютерной информации;

5. Выявление проблем в квалификации преступлений в сфере безопасности компьютерной информации, совершенной в соучастии, при неоконченной преступной деятельности, а также при наличии множественности преступлений.

6. Формулирование выводов по теме дипломная работы, а также предложений по совершенствованию уголовного законодательства, предусматривающего ответственность за преступления в сфере компьютерной информации и практики его применения.

Объектом исследования являются совокупность общественных отношений, возникающих в связи с совершением преступлений против компьютерной безопасности.

Предметом дипломной работы являются Конституция Российской Федерации, нормы действующего отечественного и зарубежного уголовного законодательства, предусматривающие ответственность за преступления в сфере компьютерной информации; нормы иных отраслей российского права, регулирующие правовые отношения в сфере использования, передачи, модификации и безопасности компьютерной информации; уголовно-правовая доктрина в изучаемой сфере; статистический данные МВД России о количестве и динамике преступлений в сфере компьютерной информации; следственная и судебная практика по делам о преступлениях в сфере компьютерной информации.

К методологическим основам исследования относятся такие методы научного познания, как: диалектический метод, сравнительно-правовой (компаративный) метод, сравнительно-правовой метод, интегральный метод, ситуационный метод, формально-логический метод, историко-правовой метод.

Теоретической основой дипломной работы явились труды отечественных и зарубежных авторов, таких как: Батурин Ю.М., Бегишев И.Р.,

Беришвили Р.Ш., Гайфутдинов Р.Р., Леонтье Б.К., Минаев С.В., Чакрян В.Р., Щепельков В.Ф и др.

Эмпирической основой дипломной работы явились статистические данные о количестве и динамике компьютерных преступлений, совершенных в России в период с 2020 по 2024 годы; материалы следственной и судебной практики по делам о преступлениях в сфере компьютерной информации, рассмотренных, рассмотренных судами Российской Федерации.

Нормативной основой исследования стали Конституция Российской Федерации, международно-правовые акты в сфере охраны компьютерной информации, Уголовный кодекс Российской Федерации, Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», иные федеральные законы и подзаконные нормативно-правовые акты в сфере охраны компьютерной информации, уголовные законодательства Германии, Нидерландов, Ирландии.

Научно-практическая значимость исследования определяется, прежде всего, возможностью использования сформулированных в выпускной квалификационной работе выводов в практике следственных и судебных органов при преодолении пробелов в праве, а также решении вопросов квалификации этих преступлений и отграничении их от новых составов преступлений. Кроме того, исследование темы позволит по-новому взглянуть на отечественное и зарубежное законодательство, воспринять их историю и развитие. Результаты работы могут быть использованы юристами, судьями, специалистами в области компьютерных технологий, поскольку многие приводимые в исследовании данные малоизвестны или неизвестны вообще в России из-за отсутствия источников на русском языке.

Научная новизна выражается в формулировании предложений по совершенствованию действующего уголовного законодательства,

предусматривающего уголовную ответственность за преступления в сфере компьютерной информации:

1. Обоснована целесообразность изменения наименования главы 28 УК РФ на: «Преступления против безопасности компьютерной информации».

2. Предложено авторское определение термина «киберпреступность». В рамках данной дипломной работы под киберпреступностью мы понимаем совокупность всех преступлений, в рамках которой используются либо атакуются компьютер, компьютерная сеть или отдельно взятое сетевое устройство.

3. Обоснована необходимость привлечения к уголовной ответственности пользователей искусственного интеллекта, используемого с целью совершения преступлений.

4. Изложить ч. 1 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в следующей редакции:

Доступ к охраняемой компьютерной информации, если это деяние повлекло неправомерно удаление, блокирование, модификацию либо копирование компьютерной информации, - …» далее по тексту;

5. Использовать для целей применения уголовного закона только понятие «Компьютерное устройство», без использования понятия «ЭВМ».

Апробация результатов исследования. Основные положения работы отражены в опубликованных автором научных статьях, а также докладывались на Всероссийских, межвузовских конференциях.

1. Цифровая валюта (криптовалюта) как новый предмет преступления // Всероссийская научно-практическая конференция аспирантов и студентов ВУЗов России, адъюнктов, курсантов и слушателей образовательных организаций МВД России «Теория и практика противодействия преступности уголовно-правовыми средствами». – Казань: КЮИ МВД России, 20.05.2021.

2. Киберпреступление: понятие, содержание и меры противодействия // Всероссийский круглый стол на тему: «Дистанционные хищения и кибербезопасность». – Казань: КЮИ МВД России, 22 марта 2023 г.

3. Уголовно-правовое противодействие компьютерным преступлениям // Всероссийский научно-практический семинар. – Казань: КЮИ МВД России, 5 мая 2023 г.

4. Проблемы квалификации преступлений в сфере компьютерной информации // Межвузовская научно-практическая конференция курсантов, студентов и слушателей на тему «Уголовное и уголовно-исполнительное законодательство: вчера, сегодня, завтра». – Казань, КЮИ МВД России, 6 июня 2024 г.

5. Современные практики совершения мошенничества с использованием средств платежей // VI Всероссийский круглый стол «Выявление, раскрытие, и расследование преступлений, совершаемых в сфере оборота электронных платежных средств». – Казань, КЮИ МВД России, 2025

6. Дистанционные хищения и их уголовно-правовое противодействие // Всероссийский научно-практический круглый стол «Дистанционные хищения и кибербезопасность». – Казань, КЮИ МВД России, 2025

7. Тенденции развития мошенничества: новые технологии, взлом систем безопасности, использование искусственного интеллекта // V Республиканская научно-практическая конференция «Финансовая грамотность: опыт, пробелы, вызовы» – Казань, КЮИ МВД России, 2025

8. Уголовная ответственность за компьютерные преступления: проблемы применения норм уголовного законодательства // Ежегодная межвузовская научно-практическая конференция «Уголовное и уголовно-исполнительное законодательство: вчера, сегодня завтра» - Нижний Новгород, Нижегородская академия МВД России, 25 мая 2025.

Структура дипломной работы обусловлена её целью и задачами, и включает в себя: введение, три главы, объединяющие девять параграфов, заключения и списка используемой литературы.

ГЛАВА 1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§1 Понятие, сущность информации и компьютерной информации

Термин «информация» произошел от латинского слова «informatio» и переводится как представление о чем-либо[1]. Из этого следует, что это какие-либо сведения об окружающей действительности, передаваемые между людьми вне зависимости от способа фиксации таких сведений. На протяжении всей своей истории «информация» коренным образом меняла свою форму. Но ключевые перемены значения произошли в послевоенный период – середина XX века.

Само определение приобрело свое новое значение в 1948 году. Именно в этом послевоенном году вышла в свет книга известного американского математика и основоположника кибернетики Норберта Винера. Видный ученый приходит к выводу, что информация начинает считаться третьим основным понятием природы наряду с материей и энергией.

В то же время Клод Шеннон, основоположник и «отец» информационного века ввел понятие бита как единицы измерения количества информации. Именно он высказывается о том, что «информация» начинает считаться самостоятельной единицей, имеющий свой вес объем. Так им была придумана первая единица измерения информации в ее цифровом значении – бит. Впоследствии он приходит к выводу, что отныне «информацию»

[1]Большой толковый словарь русского языка URL: - https://gramota.ru/poisk?query=информация&mode=slovari&dicts[]=42 (дата обращения 01.03.2025).

необходимо измерять цифровом эквиваленте, тем самым породив информационную эру.

В дальнейшем коллега Шеннона, Уоррен Уивер, ученый и математик, предоставляет уточнение, что в рамках разработанной совместной теории слово «информация» используется в качестве единицы передаваемого цифрового сигнала. И не всегда такой сигнал будет иметь смысл. Все это выльется в основу концепции как обработки информации и распространение информационных технологий.

На протяжении всего XX века происходило изучение, осознание теории компьютерной информации. Широкое распространение получили промышленные электронно-вычислительные машины (далее по тексту – ЭВМ), прототипы современных персональных компьютеров (далее по тексту ПК). Человечество все дальше устремлялось вперед, в свое светлое цифровое будущее. Однако свою полную силу цифровизация обретет только в XXI веке.

В Российской Федерации цифровизация начинается в 90-е годы. Стремительными темпами по нашей стране прокатиться демократизация. Вместе с ней расширяться международные связи. Все это приведет к тому, что Россия будет подключена к «всемирной паутине» - сети Интернет. В связи с распространением, хоть и не повсеместным, компьютеров, которыми будут также пользоваться и государственные органы, и силовые структуры и в целом гражданами, начинается особая версия переноса данных на более современные девайсы, возникает острая необходимость защиты таких данных. Причем не только с технической точки зрения, но в первую очередь именно с правовой. С распространением персональных компьютеров, тех же самых примитивных ЭВМ, появляется первой виток новых преступлений, впоследствии названных киберпреступлениями (по сей день остаются одними из наиболее латентных). Киберпреступность в широком смысле классифицируется по признаку роли в правоотношении персонального

компьютера и сети Интернет[1]. Поэтому преступления направлены против компьютера, выступающего хранилищем какой-либо информации и/или персональных данных, интернет-сети в целом или же совершенные с использованием как компьютера, так и «всемирной паутины». Отличительной особенностью является тот факт, что все они затрагивают именно нематериальный, цифровой элемент информационных потоков и различных данных. Особым дополнением к таким преступлениям выступает создание различных программ-вирусов, названные в дальнейшем законодателем вредоносными компьютерными программами.

Следует также отметить, что в 2000 году в ходе заседания ООН по вопросам предупреждения преступлений и привлечению к ответственности киберпреступников сами киберпреступления были разбиты на пять основных категорий: Неправомерный доступ к компьютерной информации; 1. Повреждение или уничтожение компьютерной информации или нарушение работы программ; 2. Нарушение функциональности работы компьютерной системы или целостности сети; 3. Несанкционированный перехват данных внутри системы или сети; 4. Компьютерный шпионаж (с использованием вирусных программ).

Именно поэтому отечественные законодатели пришли к выводу о необходимости определения ответственности за совершения таких преступлений. Возникает новая глава Уголовного кодекса Российской Федерации, а именно «Преступления против компьютерной информации».

В науке уголовного права высказывается точка зрения о том, что следует различать взаимосвязанные между собой понятия «информационная безопасность», «компьютерная безопасность», «защита информации» и «безопасность информации». При этом компьютерная безопасность рассматривается автором как одна из составляющих информационной

[1] Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. 159 с. URL: https://spblib.ru/ru/catalog/-/books/11477840-komp-yuternaya-prestupnost-i-komp-yuternaya-bezopasnost- (дата обращения 16.03.2025).

безопасности наряду с иными элементами поддерживающей ее инфраструктуры. К ним относятся жилищные, коммунальные системы, системы жизнеобеспечения, средства коммуникации и др. При таком подходе содержание понятия «информационная безопасность» включает в себя компьютерную безопасность[1].

На законодательном уровне понятие «информация» дается в Федеральном законе от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., вступ. в силу с 01.01.2025) в ст. 2. Так, под информацией принято понимать - сведения (сообщения, данные) независимо от формы их представления[2].

Понятие компьютерной информации дается в примечании к ст. 272 УК РФ это - сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

Информация, в качестве сведений, включает в себя: персональные данные, результаты интеллектуальной собственности, банковские сведения и др. На наш взгляд, данное понятие носит слишком общий, универсальный характер. В нем нет указания на реквизиты, дающие нам понимание о том, кто является, собственника или владельца информации и т.д. Данные термины нуждаются в уяснении ряда технических характеристик новых средств обработки информации, а также сущности самой информации как уголовно-правовой категории.

---

[1] Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации // Автореф. дисс. на соиск. ученой степени канд.юрид.наук. – Казань: Изд-во Казанского (Приволжского) федерального университета, 2017. С. 8; Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика // Дисс. на соис. ученой степени докт.юрид наук. М.: Изд-во института Прокуратуры РФ, 2011. С. 276; 53. Капырюлин А.А. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический апекты // Дисс. на соис. ученой степени докт.юрид наук. – Тамбов, 2007. С. 12.

[2] См.: об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 23.11.2024) (с изм. и доп., вступ. в силу с 01.01.2025) // СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения 01.02.2025).

В связи с этим, для целей уголовного закона, под компьютерной информацией, как предмета преступления мы предлагаем понимать - организационно упорядоченную совокупность сведений (сообщений, данных), зафиксированных на машинном носителе либо в информационно-телекоммуникационной сети с реквизитами, позволяющими их идентифицировать, имеющую конкретного собственника либо иного законного владельца, в том числе созданную с помощью технологий искусственного интеллекта.

Сюда же следует отнести и технологии искусственного интеллекта, которые последнее время столь активно используются. Они заслуживают такого внимание прежде всего из-за того, что большинство их алгоритмов построено на активном анализировании, использовании и применении компьютерной информации.

В силу отсутствия человеческого фактора в виде ограниченных человеческих возможностей, реальный потенциал искусственного интеллекта представляется безграничным.

Выходит, что человеком придумана сверхтехнология для систем, машин и компьютеров, позволяющая выполнять такие задачи, которые ранее требовали разумного мышления, то есть исключительно человеком. Впоследствии была добавлена функция самосовершенствования и самообразования, информацию получив при этом из всех доступных информационно-телекоммуникационных сетей, а также из сети Интернет.

Искусственный интеллект использует алгоритмы, которые позволяют компьютеру обрабатывать большие объёмы данных и находить в них закономерности. На основе этих закономерностей он может делать выводы, предсказывать события или принимать решения. Именно этот аспект в настоящее время активно используется злоумышленниками для своей преступной деятельности.

Так, в самом начале развития этого интеллекта, преступники активно начали пользоваться существующими уязвимостями, что позволило им проще

совершать преступления – получать конфиденциальную информацию, находить нужные вредоносные программы для своих целей и т.п. Все это привело к тому, что искусственный интеллект стал подробно расписывать план совершения преступления, в какое время лучше совершать, какие при этом использовать средства и орудия.

Так продолжалось не долго, и разработчиками были внесены корректировки в поведение искусственного интеллекта, в которых были четко прописаны правила и порядок реагирования на такие запросы.

Однако из-за произошедших утечек, в руки компьютерных гениев преступного мира попали технологии создания таких «программ-помощников», после создания которых те стали активно загружаться в сеть «Даркнет». К сожалению, полностью взять под контроль технологию искусственного интеллекта практически невозможно. Безусловно такие технологии облегчили нашу повседневную жизнь, но они же подвергают риску наше цифровое пространство.

§ 2. Понятие, сущность и система преступлений в сфере компьютерной информации

Термин «компьютерное преступление» впервые появился в зарубежной литературе в начале 60-х годов прошлого века, когда стали регистрироваться случаи совершения преступлений с использованием компьютера.

На законодательном уровне понятие компьютерных преступлений не сформулировано. В то же время, в теории уголовного права существует множество определений данного понятия. Часто используют словосочетания «компьютерные преступления», «преступления в сфере компьютерной информации», «преступления в сфере компьютерных технологий» и др.

Так, например, под компьютерными преступлениями понимают – любого рода незаконное или неразрешенное поведение, которое воздействует на автоматизированную обработку и передачу данных[1].

Компьютерные преступления — это действия, совершаемые с целью получения и использования информации в компьютерной сфере. А компьютерная информация может быть, как предметом, так и средством совершения преступления[2].

К «компьютерным преступлениям» относятся любого рода преступления, связанные с компьютерной техникой, которые при этом противоречат праву[3]. По мнению Бекряшева А. К. под компьютерным преступлением следует считать незаконное и неразрешенное поведение, которое тесно соприкасается с обработкой и передачей данных[4].

Под компьютерными преступлениями выделяют опасные действия, предусмотренные уголовным законом, в которых информация ЭВМ является объектом преступления[5].

Под преступлением в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства.

К преступлениям в сфере информационных технологий можно отнести как распространение вредоносных программ, взлом паролей, кражу номеров

---

[1] Беришвили Р.Ш., Чакрян В.Р. Компьютерные преступления // Международный научный журнал «Символ науки» № 12-1 / 2021. С. 53.

[2] Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы. – М.: Майор (Осипенко), 2001 – 190 с. Текст: электронный URL: https://lib.ru/TECHBOOKS/LEONTIEV/hakery.txt (дата обращения 22.03.2025)

[3] Седаков С.Ю., Филиппова Т. П. Хрестоматия по всеобщей истории государства и права. М.: Юрист, 1996. С. 20.

[4] Бекряшев А. К., Белозеров И. П. Теневая экономика и экономическая преступность, 2003. 149 с. Текст: электронный //URL: https://knigogid.ru/books/1907184-tenevaya-ekonomika-i-ekonomicheskaya-prestupnost/toread (дата обращения 28.03.2025)

[5] Минаев С. В. Компьютерные преступления: сущность, особенности и возможности предотвращения // NOMOTHETIKA: Философия. Социология. Право. 2017. №24 (273). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya (дата обращения: 09.05.2025).

банковских карт и других банковских реквизитов, так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т.д.) через Интернет, а также вредоносное вмешательство через компьютерные сети в работу различных систем.

Как предполагают многие отечественные и зарубежные специалисты, следует выделить две главных точки зрения научной мысли по данному вопросу. Белозеров И.П. и Копырюлин, А.Н. к компьютерным преступлениям относят преступления, где непосредственно ЭВМ является, как орудием для покушения на чью-то информацию, так и объектом, с целью получения выгоды и нанесению ущерба другой стороне. А хищение ЭВМ само собой рассматривается как один из путей осуществления преступлений в компьютерной среде. Батурин Ю.М. и Жодзишский А.М. относят к компьютерным преступлениям только действия в сфере автоматизированной обработки информации, направленные против закона[1].

Понятие «компьютерные преступления» многозначно и не имеет точного определения. Оно может употребляться:

- В качестве синонима понятия «преступления в сфере компьютерной информации»;
- Выступать в виде определения преступлений, которые совершаются непосредственно в информационно-телекоммуникационной сфере;
- Как совокупность преступлений, которые могут совершаться с помощью компьютера, смартфона и прочего оборудования, компьютерной системы или сети, в рамках компьютерной системы или сети, против тех же компьютеров, компьютерных систем и сетей.

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

[1] Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. – С. 112.

компьютерной информации, информационные компьютерные преступления и киберпреступления.

Рассматриваемую в работе группу преступлений (ст. ст. 272-2741 УК РФ), на наш взгляд, следует именовать как «преступления против безопасности компьютерной информации», под которыми следует понимать запрещенные уголовным законом РФ виновно совершенные общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности обращения (производства, хранения, использования либо распространения) компьютерной информации или вреда критической информационной инфраструктуре Российской Федерации (далее – КИИ РФ). В предлагаемом определении словосочетание «в сфере» (указанное в УК РФ) целесообразно заменить другим - «против безопасности». Такая необходимость обусловливается системной структурой Особенной части УК РФ, в котором все посягательства на видовые объекты (за исключением двух, среди которых и анализируемые в работе преступления) определены через термин «против». Ибо безопасность компьютерной информации является конкретно определенным объектом уголовно-правовой охраны в отличие от всеобъемлющего понятия «сфера компьютерной информации». Более того, в процессе совершения данных деяний вред причиняется безопасности отношений в сфере компьютерной информации, следовательно, использование данного термина более логично.

Основным классифицирующим признаком компьютерных преступлений является общность методов, средств, объектов посягательства. Объект посягательства — это информация, обрабатываемая в компьютерной системе, а компьютер служит инструментом посягательства.

К этой группе компьютерных преступлений примыкают преступления, в которых украденная информация является средством попытки атаковать

другой объект уголовно-правовой защиты[1]. В связи с этим, выделяют преступления, которые совершаются с использованием компьютера:

1. Преступления, совершаемые с применением компьютера:

– компьютерные преступления против государственной власти (государственная измена (ст. 275 УК РФ), шпионаж (ст. 276 УК РФ), разглашение государственной тайны (ст. 283 УК РФ);

– компьютерные преступления экономического характера (кража, мошенничество, хищение предметов, которые имеют особую ценность и др.);

– компьютерные преступления против общественной безопасности и общественного порядка (заведомо ложное сообщение об акте терроризма (ст. 207 УК РФ), сокрытие информации об обстоятельствах, создающих опасность для жизни или здоровья людей, общества (ст. 237 УК РФ);

– компьютерные преступления против личности (ст. клевета (ст. 128.1 УК РФ), нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений (ст. 138 УК РФ).

Основным классифицирующим признаком компьютерных преступлений является общность методов, средств, объектов посягательства.

В зависимости от способа воздействия на компьютерную систему специалисты выделяют несколько видов компьютерных преступлений:

• Физические злоупотребления, которые включают в себя деструкцию оборудования, как частичное повреждение, так и полное уничтожение ценных информаций.

• Операционные злоупотребления, чаще всего: подмена носителей и считывающих устройств, выдача себя за другое лицо путём мошенничества.

• Программные злоупотребления, из-за которых может измениться работа всей системы, но данную неполадку можно будет обнаружить только спустя определённое время[2].

---

[1] Гриб Г.В., Тюнис И.О. Криминалистика и цифровые технологии: научный журнал / Российский следователь, 2020. – №9. – С. 156 – 160.

[2] Батурин Ю. М. Проблемы компьютерного права. - М.: Юриздат, 1991. С. 45.

Некоторые авторы предлагают систему компьютерных преступлений, в которой можно выделить две большие категории:

- Преступные действия, направленные на дестабилизацию работы компьютеров, информационно-телекоммуникационных сетей, элементов сети Интернет и т.п;
- Преступления, совершенные путем использования компьютеров, смартфонов и иных видов электроники в качестве технических средств[1].

Волеводзом А.Г. была предложена классификация, построенная на признаке объекта преступлений:

- Преступления, непосредственно посягающие на отношения в сфере компьютерной информации;
- Преступления, посягающие отношения по поводу реализации прав на информационные ресурсы, информационную инфраструктуру и отдельные её части;
- Преступления против личных прав и частной сферы[2].

На наш взгляд, наиболее полной и оптимальной является система преступлений, в сфере компьютерной информации, которая включает в себя следующие виды преступлений:

• Незаконный доступ к компьютерной информации (ст. ст. 272-272[1] УК РФ).

• Преступления, направленные на осуществление незаконных действий, путём создания, распространение и (или) использование компьютерных программ (ст. 273- 274[2] УК РФ).

• Преступления, связанные с неправильной эксплуатацией и управлением компьютерной информацией и информационно-телекоммуникационными сетями (ст. 274 УК РФ).

---

[1] Чакрян В.Р. «Классификация преступлений» Научная электронная библиотека «КиберЛенинка» https://cyberleninka.ru/article/n/ponyatie-kompyuternyh-prestupleniy-i-ih-klassifikatsiya/viewer (дата обращения 09.05.2025)

[2] Волеводз А. Г. «Конвенция о киберпреступности: новации правового регулирования https://mgimo.ru/library/publications/113908/?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru (дата обращения 09.05.2025)

Общественная опасность противоправных действий в области электронной техники и информационных технологий выражается в том, что они могут повлечь за собой нарушение деятельности автоматизированных систем управления и контроля различных объектов, серьезное нарушение работы ЭВМ и их систем, несанкционированные действия по уничтожению, модификации, искажению, копированию информации и информационных ресурсов, иные формы незаконного вмешательства в информационные системы, которые способны вызвать тяжкие и необратимые, в том числе тяжкие последствия.

§ 3. История развития уголовного законодательства об ответственности за преступления в сфере компьютерной информации в Российской Федерации и зарубежных странах

Впервые в Российском уголовном законодательстве ответственность за совершение компьютерных преступлений появилась с принятием УК РФ 1996 года. Изначально в тексте УК РФ было всего 3 преступления, предусмотренные статьями 272, 273 и 274 УК РФ. Была установлена уголовная ответственность за неправомерный доступ к компьютерной информации, создание, использование и распространение вредоносных компьютерных программ, нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Позже, Федеральным законом от 26.07.2017 N 194-ФЗ[1] была введена ст. 274[1] УК РФ, предусматривающая ответственность за

[1] О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона О безопасности критической информационной инфраструктуры РФ: Федеральный закон от 26.07.2017 N 194-ФЗ СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 09.05.2025)

неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Далее, в 2022 году Федеральным законом от 14.07.2022 N 260-ФЗ[1] была введена ст. 274[2], в которой лицо подвергалось уголовной ответственности непосредственно за 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 2024 году был принят Федеральный закон от 30.11.2024 N 421-ФЗ[2], в котором в УК РФ была внесена статья 272[1], согласно который лицо подлежит уголовной ответственности при незаконном использовании и (или) передаче, сборе и (или) хранении компьютерной информации, содержащей персональные данные, а равно создание и (или) обеспечение функционирования информационных ресурсов, предназначенных для ее незаконных хранения и (или) распространения.

Само явление киберпреступности не осталось незамеченным ни в одной из стран. Конечно же, назревшие реформы уголовного законодательства также незамедлительно последовали. Для полного и всеобъемлющего анализа данного преступления необходимо рассмотреть трактование компьютерных преступлений в уголовном законодательстве стран Запада и сравнить с УК РФ.

Первый законопроект, определяющий уголовную ответственность за преступления в сфере компьютерной информации, был разработан в США еще в далеком 1977 году и выступил в будущем базой для дальнейшей регламентации и квалификации преступных деяний в сфере компьютерной,

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 N 260-ФЗ (последняя редакция) СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/3d0cac60971a511280cbba229d9b6329c07731f7/

[2] О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30.11.2024 N 421-ФЗ https://www.consultant.ru/document/cons_doc_LAW_491931/

цифровой информации. На его основе в октябре 1984 года был принят закон о мошенничестве с использованием компьютеров - ключевой законодательный акт, определяющий уголовную ответственность за преступления в сфере цифровой информации. В дальнейшем в связи с появлением все новых способов он постоянно дополнялся.

Данный уголовный закон установил уголовно-правовую ответственность за несколько базовых составов преступлений:

- Шпионаж с использованием технических средств - компьютеров;
- Получение несанкционированного доступа к цифровой информации;
- Мошенничество с использованием компьютеров и компьютерных сетей;
- Нарушение функциональности компьютеров;
- Взлом государственных защищенных сетей;
- Вымогательство;
- Интернет-шантаж[1].

В самом начале наказание за такие деяния разнились, принимались различные денежные взыскания, а за более тяжкие предусматривалось тюремное заключение.

В последние годы Конгресс США рассматривает новый законопроект о кибербезопасности, который предусматривает ужесточение наказания за совершенные деяния. Следует также отметить, что с 2003 года основные обязанности по обеспечению защищенности киберпространства США возложены на Министерство внутренней безопасности.

Так, один из разделов закона посвящен шпионажу в экономической сфере и предусматривает повышенные штрафы за кражу интеллектуальной собственности именно американских компаний (отчетливо просматривается политика протекционизма). В этом разделе установлены сроки лишения

[1] Крылова Н. Е. Уголовное право зарубежных стран. Особенная часть: учебник для вузов / ответственный редактор Н. Е. Крылова. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 397 с. — (Высшее образование). — ISBN 978-5-534-16218-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561346 (дата обращения 07.03.2025)

свободы, они могут составлять 20 лет. Если же преступник взломал защищенные компьютерные сети инфраструктуры США – объекты критической инфраструктуры – телекоммуникационные сети, энергосети, закрытые каналы связи, системы управления водоснабжением и т.д., то срок лишения свободы может составлять 30 лет, причем с особой оговоркой - без права на условно досрочное освобождение.

В силу развитой децентрализации, отдельные штаты вправе самостоятельно принимать уголовные законы за киберпреступления. Отдельные прецеденты принятия таких законов просматриваются в штате Калифорния.

Что касается другой англосаксонской страны – Великобритании, то в августе 1990 года был принят «Акт о компьютерных злоупотреблениях»[1]. Первый параграф посвящен осуществлению неправомерного использования компьютера. Данный по своей сути уголовный закон определял, что лицо считается виновным в совершении преступления, когда оно использует компьютер для получения доступа к любой программе или данным, находящимся на другом компьютере. Затем было добавлено уточнение, что преступлением данное деяние будет считаться только в том случае, если происходит изменение или уничтожение данных, их копирование или искажение, и наказание выражалось в виде назначения штрафа или лишения свободы на 6 месяцев[2].

В связи с ростом террористической угрозы в мире и при всей серьезности проблемы компьютерных преступлений в 2000 году был разработан и принят «Закон о терроризме». В нем определение терроризма было расширено и стало затрагивать киберпространство.

---

[1] Computer Misuse Act 1990: call for information – Акт о компьютерных злоупотреблениях Великобритании https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information (дата обращения 06.03.2025)

[2] Голованова, Н. А. Уголовное право Англии: учебник для вузов / Н. А. Голованова. — Москва: Издательство Юрайт, 2025. — 188 с. — (Высшее образование). — ISBN 978-5-9916-8869-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561351 (дата обращения 06.03.2025).

Что касается стран романо-германской правовой семьи, то для строгой квалификации деяния в немецком уголовном кодексе был введен термин «daten», означающий, что правовой защите подлежат данные, которые находятся и хранятся на цифровом носителе, т.е. компьютерные данные.

Также был разработано и принят 27 раздел Уголовного кодекса ФРГ[1], который отчасти схож с главой 28 нашего Уголовного кодекса. Однако если в отечественном законодательстве все строго упорядочено, и вся глава посвящена преступлениям в сфере компьютерной информации, то в немецком отражено несколько статей, причем только в нескольких статьях объектом выступают данные в их цифровом виде. Соответственно, наказание последует за их изменение повреждение, удаление и сокрытие. Причем законодатель ссылается на положение статьи, которая была описана абзацем выше.

Кроме того, в немецком законодательстве нашел отражение компьютерный саботаж, включающий в себя и создание вредоносных программ. Посвященная этому статья содержит положения о том, что такими деяниями признаются вмешательство в процесс обработки какой-либо компьютерной информации, которая является критически важной для функционирования предприятия, государственной корпорации, государственному органу и т.д.[2] В УК РФ существует аналог такому деянию - статья 281 – диверсия, однако четкое понимание цифровой сферы данного деяния еще до сих пор отсутствует. Хотя в последние годы попытки совершить диверсии на информационное поле РФ кратно возросли.

Нидерланды входят в десятку стран с самым высоким процентом пользователей сети Интернет – 94,4% от населения страны. Поэтому вопрос

---

[1]Уголовный кодекс Федеративной республики Германии https://www.uni-potsdam.de/fileadmin/projects/ls-hellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB-%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf (дата обращения 06.03.2025)

[2] Серебренникова А. В. Уголовное право Германии: учебник для вузов / А. В. Серебренникова. — Москва: Издательство Юрайт, 2025. — 124 с. — (Высшее образование). — ISBN 978-5-534-10123-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561354 (дата обращения 09.03.2025)

компьютерных преступлений считается одним из главных в данной стране. Нидерланды в вопросе обеспечения компьютерной безопасности вначале 1990-х создали Консультативный комитет по компьютерным преступлениям - аналог ФСТЭК России.

Таким образом, компьютерным преступлением признается совершенное исключительно умышленно, с целью получения выгоды, включающее использование лицом или лицами какой-либо технической аппаратуры для перехвата или записи компьютерной информации, находящейся в телекоммуникационной системе или сети Интернет. Помимо этого, лицо, предоставившее аппаратуру для незаконного получения компьютерной информации, протекающих по телекоммуникационным или автоматизированным системам.

Однако хоть и виды наказания в нашем УК РФ и УК Нидерландов совпадают, но отличаются их суровостью – УК Нидерландов предусматривает меньший размер штрафа, а в отдельных случаях наказание в виде лишения свободы не превышает 6 месяцев[1].

В целом, УК Нидерландов, предусматривает ответственность за совершение основных преступлений, описанных в законодательстве других стран.

В Ирландии же ответственность за преступления против компьютерной информации предусмотрены принятым в 1991 году «Актом о криминальном ущербе»[2]. В нем указано, что лицо, использующее компьютер с намерением получить неправомерный доступ к данным на цифровом носителе, будет признано виновным в совершении преступления вне зависимости оттого, удалось ли получить эти данные.

Стоит отметить, что самый близкий значению к УК РФ оказался УК ФРГ, имеющий похожие диспозиции статей о привлечении лица к уголовной ответственности за компьютерные преступления. Однако в российское

---

[1] Уголовный кодекс Нидерландов Официальный сайт Правительства Нидерландов // URL: https://www.government.nl/ (дата обращения 06.03.2025)

[2] Уголовный кодекс Ирландии Официальный сайт Правительства Великобритании // URL: https://www.legislation.gov.uk/apni/1966/20/section/8 (дата обращения 06.03.2025)

уголовное законодательство следует добавить статью именно о компьютерном саботаже, которая весьма актуальна последние года.

В ходе рассмотрения первой главы были затронуты основные понятия, историческая справка и проведен анализ законодательств развитых стран. Компьютерная информация заменила примитивные способы фиксации данных, а с середины 70-х годов прошлого века начался путь цифровизации как общественных отношений, так и в общества в целом. Появления первых компьютеров, а вслед за ними первых преступлений как раз таки свидетельствуют об этом. Все это неизбежно привело к развитию уголовного законодательства в этом направлении.

В дальнейшем компьютерные преступления стали носить межгосударственный характер. Все это привело к необходимости создания условий для раскрытия данных преступлений – в отдельных странах были созданы специальные государственные органы, отвечающие за безопасность в этой сфере.

Помимо этого, с уверенностью можно заявить, что в законодательствах стран Запада просматривается единоначалие в подходах к определению сути преступления против компьютерной информации. Западные законодатели строго регламентировали подход к пониманию данного деяния, указали в действующих уголовных законодательствах аспекты, на которые стоит обратить внимание.

В силу того, что в РФ активный процесс цифровизации начался только лишь в 2010-х годах, явно просматривается проблематика отдельных статей Уголовного кодекса. Действующие комментарии и постановления Пленума Верховного суда не помогают в полной мере раскрыть суть деяния. Отдельные положения главы 28 уже устарели, следует их изменить, доработать, ввести новые статьи в силу действующих реалий, а некоторые и вовсе вывести. Однако стоит похвалить уголовное законодательство за строгость наказаний в отличие от тех же самых стран Запада. Стоит еще отметить, что каждое виновно совершенное общественно-опасное деяние полагается рассматривать в совокупности всех его частей: как объективной стороны, так и субъективной.

В силу этого предлагается перейти к рассмотрению второй главы данной работы.

ГЛАВА 2. ЮРИДИЧЕСКИЙ АНАЛИЗ СОСТАВОВ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Объективные признаки составов преступлений, предусматривающих ответственность за преступления в сфере компьютерной информации

Объектом преступления выступают общественные отношения, которым причиняется ущерб совершением преступления. Чаще всего объектом выступают социальные ценности, права, свободы и законные интересы человека, предметы материального мира и иные ключевые аспекты повседневной жизни людей.

По своей сути, основные объекты преступления, которые подлежат защите, отражены в статье 2 УК РФ: охрана прав и свобод человека и гражданина, собственности, общественного порядка и общественной безопасности, окружающей среды, конституционного строя Российской Федерации от преступных посягательств, обеспечение мира и безопасности человечества, а также предупреждение преступлений. Таким образом, законодатель, исходя из задач УК РФ, перечислил основные объекты.

Забегая немного вперед, преступления в сфере компьютерной информации посягают на частную жизнь граждан, их персональные данные, которые не должны находиться в публичном доступе. Однако к таким преступлениям российские законодатели еще отнесли и распространение программ-вирусов, атаки на информационную инфраструктуру РФ (в них объект будет отличен от 272 и 272^1 статей УК РФ). Глава 28 давно требует доработки и конкретизации отдельных деяний. Помимо этого, считается необходимым ужесточить наказание за совершение преступлений, составы которых отражены в данной главе. Вернемся к проблемам этой главы позже.

Делая небольшой вывод, объект преступления – это такие отношения, которые обладают следующими чертами:

- Представляют собой общественные отношения;
- Находятся под охраной уголовного закона;

- Им, в результате совершения преступления, причиняется вред или создается угроза причинения вреда, т.е. присутствует конкретность.

Объект преступления находит отражение в Особенной части кодифицированных уголовно-правовых актов: преступления в них могут группироваться по разделам и главам по признаку родового объекта преступления. Объект преступления рассматривается в числе элементов состава преступления[1].

Основное значение объекта преступления определяется его ролью в структуре состава преступления, а также наличием в определении преступления материального признака: не может быть преступлением деяние, не причиняющее вреда и не создающее угрозы причинению вреда объектам уголовно-правовой охраны; соответственно, если не установлено, какому объекту причиняет вред конкретное преступление, либо если причинённый вред является малозначительным, не может идти речи о преступности деяния: нет преступления без объекта посягательства. Материальным признаком, на основе которого устанавливается объект преступления, являются причинённые им общественно опасные последствия[2].

Объект преступления позволил удобно кодифицировать отечественное законодательство. Структура Особенной части УК РФ построена как раз по признаку общности объектов определённой группы преступлений.

Опираясь на объект преступления можно производить разграничение преступлений при их квалификации. Кроме этого, установление причинения существенного вреда объекту уголовно-правовой охраны позволяет отграничить преступления от правонарушений и аморальных проступков.

---

[1] Векленко В. В. Уголовное право. Общая часть: учебник для вузов / под общей редакцией Векленко В. В. — 3-е изд. — Москва: Издательство Юрайт, 2025. — 512 с. — (Высшее образование). — ISBN 978-5-534-15530-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562995 (дата обращения 27.03.2025).

[2] Боровиков, В. Б. Уголовное право. Общая часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов; под редакцией В. Б. Боровикова. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 243 с. — (Высшее образование). — ISBN 978-5-534-19802-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561008. (дата обращения 24.03.2025).

Традиционно выделяется вертикальный способ классификации объектов: общий, родовой и непосредственный и по горизонтали: основной, дополнительный и факультативный. В отличие от уголовных кодексов иностранных государств, в российском уголовном праве выделяется также видовой объект.

Общий объект представляет собой совокупность общественных отношений, на которую посягает любое общественно опасное деяние. Содержание данного вида объекта представляет собой все блага, которые признаются наиболее значимыми[1].

Родовой объект (также называемый «специальным») является характерным только для определённой группы преступлений. По своей сути он представляет собой такую группу схожих общественные отношения, на которые посягает ровно такая же группа однородных преступлений. Родовыми объектами являются, например, личность, собственность, интересы правосудия и т.д. Именно родовой объект служит для разграничения сходных по составу преступлений. Таким образом, родовым объектам по УК РФ соответствует раздел Особенной части. Соответственно, в главе 28 УК РФ родовым объектом выступают общественные отношения, общественная безопасность и общественный порядок сообразно разделу.

Видовой объект представляет собой часть родового объекта, объединяющая уже более узкие группы общественных отношений, отражающих единый интерес участников этих отношений или же выражающих некоторые тесно связанные интересы одного и того же объекта. Он соотносится с родовым объектом как часть с целым, как вид с родом. Видовой объект объединяет группу общественных отношений, вследствие чего каждое общественное отношение становится непосредственным объектом при совершении преступления, относящегося к данному виду.

---

[1] Медведев, Е. В. Уголовное право России. Общая часть: учебное пособие для вузов / Е. В. Медведев. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 221 с. — (Высшее образование). — ISBN 978-5-534-18080-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/534237. (дата обращения 09.04.2025)

Видовым объектам соответствуют главы Особенной части УК РФ. В рассматриваемом случае – преступления против компьютерной информации.

Видовой объект преступлений в сфере компьютерной информации — общественные отношения и интересы в сфере охраняемого законом обращения компьютерной информации или нормального функционирования (эксплуатации) информационно-телекоммуникационных сетей и оконечного оборудования[1].

Непосредственным объектом признается тот конкретный вид общественных отношений, которому непосредственно причиняется вред от преступного посягательства. Т.е. это объект конкретного деяния, запрещённого уголовным законом под угрозой наказания, какой-либо конкретный интерес или благо, которому посягательством причиняется ущерб. Этот объект может быть уже родового объекта или совпадать с ним, он также может быть единым для некоторой группы составов преступлений.

Основным непосредственным объектом преступлений в сфере компьютерной информации являются конкретные общественные отношения, возникающие в той или иной плоскости оборота компьютерной информации — ее создания, распространения, использования, хранения, либо доступа к ней, а также информационно телекоммуникационным сетям и оконечному оборудованию, а также включая вредоносные программы и совершения с помощью них преступлений в отношении компьютерной информации.

В качестве факультативного объекта могут выступать имущественные общественные отношения, отношения в сфере охраны жизни и здоровья людей, безопасного функционирования объектов транспорта и энергетики, охраны государственной тайны, интеллектуальных прав и т. п.

---

[1] Преступления против общественной безопасности и общественного порядка: учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — Москва: Юрайт, 2025. — 158 с. — (Высшее образование). — ISBN 978-5-534-18589-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. с. 158 — URL: https://urait.ru/bcode/563347/p.158 (дата обращения: 10.05.2025).

В качестве дополнительного объекта преступлений в сфере компьютерной информации могут выступать – собственность (например, в ч. 2 ст. 272 УК РФ, нормальное функционирование служебной деятельности, например, в ч. , личная неприкосновенность – в. ч. 2, 4 ст. 272[1] УК РФ, жизнь, здоровье и др.)

Предметом преступлений, предусмотренных ст. 272 и 273 УК, является компьютерная информация, под которой в соответствии с примечанием 1 к ст. 272 УК понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи[1].

Объективная сторона преступления представляет собой неотъемлемый компонент любого состава преступления. Данный элемент включает в себя признаки, имеющие непосредственно внешнее выражение деяния в окружающем пространстве. Некоторые законодатели за объективную сторону преступления принимают процесс совершения какого-либо общественно опасного и противоправного деяния против охраняемых законом интересов, рассматриваемый с его внешней стороны. Кроме того, отдельные ученые-правоведы полагают, что объективной стороной необходимо считать внешнее выражение деяния, которое может наблюдаться со стороны.

Как бы то ни было, для того, чтобы назвать конкретное деяние преступлением необходимо наличие двух этих элементов. Однако рассматривать их следует по отдельности для полного и всестороннего анализа позволяющее более подробно изучить каждый из них и определить его значение в общей структуре деяния.

Основными признаками объективной стороны выступают:

- Деяния в виде действия или бездействия;
- Общественно опасные последствия;

---

[1] Есаков Г. А. Российское уголовное право. Особенная часть. М.: Проспект. 2023. 656 с. Текст: электронный // URL: https://www.labirint.ru/books/989332/?ysclid=mbxq7ljy9c936175081 (дата обращения 25.04.2025)

- Причинно-следственная связь между действием/бездействием и наступившими последствиями;
- Способ, место, время, обстановка, средства и орудия совершения преступления.

Следует отметить, что изначально конкретных ранее упомянутых понятий хоть и нет, но в конкретных статьях отражена та или иная сторона.

Деяние в уголовном праве — акт осознанного поведения индивида, выраженный в виде действия (т.е. активно совершенного, внешне выраженного противоправного действия, посягающего на охраняемые уголовным законом общественные отношения) или бездействия (пассивный вид волеизъявления человека, который выражается в тот, что лицо не выполняет возложенные на него задачи и функции).

В действующем УК РФ до сих пор само понятие «деяния» не закреплено, и, соответственно, не раскрыто. Однако традиционно, как и во всех уголовных кодексах зарубежных стран, выделяются две формы деяния: преступное действие и преступное бездействие. Исходя из волевого поведения будет складываться объективная сторона такого деяния.

Деяние может быть совершено разными способами. Зачастую основным способом совершения преступлений главы 28 УК РФ является использование технических средств и различного рода электронных устройств, с помощью которых преступное лицо получает доступ к компьютерной информации. В данном случае лицо используя электронную технику и ее возможности, при наличии соответствующих знаний.

По общему правилу, вред объекту может быть причинен не только путём активного, но и путём пассивного поведения человека. Однако в силу особенностей рассматриваемой группы преступлений, совершение таких деяний путем бездействия очень редко, и такое может произойти только в статьях 272^{1}, 274 и 274^{2}, когда должностное лицо специально ничего не предприняло или в силу своей некомпетентности совершило преступное бездействие, вследствие чего наступили указанные в диспозициях статей последствия.

Другим, не менее значимым признаком объективной стороны является наступление общественно опасных последствий. Под общественно опасными последствиями понимается наступление результата в ходе совершения преступного деяния конкретного результата такого деяния. Всегда сопровождается негативными изменениями объекта, на которое было направлено деяние.

Общественно опасные последствия в уголовном праве играют ключевую роль в определении как наказания, так и квалификации самого преступления. посягательства[1].

Последствия выражаются в виде прямого ущерба (, для определения которого имеются чётко установленные критерии, так и в совокупном вреде охраняемым объектам. Отсюда следует, что последствия от совершения преступления выражаются в виде причинения ущерба компьютерной информации.

Для того чтобы считать преступлением таковым, обязательно необходимо наличие связи между совершением лицом конкретного преступного деяния и последствиями от такого деяния. В уголовно-правовой среде данный признак называется причинной связью. Т.е. реальная, фактическая связь между ранее перечисленными признаками объективной стороны, которая, по сути, является обязательной для привлечения лица к ответственности. Соответственно, должна быть упрямая связь между лицом, которое используя техническое электронное средство причинило вред, получило доступ, исказило и т.п. компьютерную информацию.

Само определение причинной связи в теории уголовного права имеет широкий характер в силу наличия достаточно большого количества теорий: теория главной причины, непосредственной причины, виновной причины,

[1] Козаченко, И. Я. Уголовное право. Общая часть: учебник для вузов / И. Я. Козаченко, Г. П. Новоселов. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 400 с. — (Высшее образование). — ISBN 978-5-534-20751-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/558681 (дата обращения 08.04.2025)

диалектико-материалистическая теория исключительной причинности, теория условий, адекватная теория.

В российском уголовном праве свое распространение получила теория причинной связи, основанная как раз таки на положениях диалектико-материалистической философии. Смысл данной теории заключается в том, что разграничены между собой сами причины, т.е. явления, непосредственно породившие последствия и условия – то, что не породило последствие, а лишь создало возможность его наступления.

Кроме основных признаков, рассмотренных ранее, объективная сторона обладает и факультативными признаками.

По российскому законодательству такими признаками признаются способ, место, время, обстановка, орудия и средства совершения преступления. Основной смысл факультативных, т.е. необязательных признаков заключается в том, что они присутствуют не во всех деяниях. Однако в отдельных случаях эти признаки бывают включены в конструкцию конкретного состава преступления, тем самым выступая в качестве обязательных или квалифицирующих признаков. Помимо этого, наличие или отсутствие таких признаков может влиять на тяжесть наказания.

Итак, самое широкое распространение среди всех факультативных признаков получил способ совершения самого преступления. Под способом совершения преступления понимается реальная совокупность используемых при его совершении приёмов и методов, последовательность совершаемых преступных действий, применения средств воздействия на предмет посягательства. Для компьютерных преступлений характерно наличие непосредственного доступа к электронному устройству, получение удаленного доступа и иные смешанные способы.

Средства и орудия совершения преступления — это предметы реальной действительности и процессы, которые используются для преступного воздействия.

При совершении преступлений в сфере компьютерной информации компьютерная и иная электронная техника выступает в роли орудия. К таким средствам относятся, например:

- Компьютеры в различных вариантах исполнения (ноутбуки, моноблоки и ПК) и прочая электронная техника (планшеты, смартфоны и прочее).
- Компьютерные комплектующие, выполняющие роль накопителей для хранения данных (жёсткие диски, твердотельные накопители, приводы оптических дисков, флэш-накопители).
- Используемые сети и технологии (беспроводные Wi-Fi сети, Bluetooth, различные стандарты связи, WiMAX и прочее).
- Программное обеспечение, находящееся в свободном, запрещённом или ограниченном обороте и имеющее различное назначение (разрешённые и бесплатно распространяемые программы, вредоносные программы и т.д.).

Также в качестве орудия преступления могут использоваться программно-аппаратные устройства, такие как скиммеры и кейлогеры.

Понятие ЭВМ по содержанию, на взгляд, слишком широкое и включает в себя любое электронное устройство, предназначенное для проведения расчетов. Им может быть калькулятор, кассовый аппарат, станок на заводе и другие сложные технические устройства, которые не являются хранителями компьютерной информации, а, следовательно, орудием компьютерного преступления. Поэтому, полагаем целесообразным использовать для целей применения уголовного закона в рамках привлечения к уголовной ответственности за преступления в сфере компьютерной информации только понятие «Компьютерное устройство», без использования понятия «ЭВМ».

Местом совершения преступления в уголовно-правовом законе принято считать объективно существующая, ограниченная территория земной поверхности, на которой совершается преступление. В качестве места совершения преступлений против компьютерной информации могут быть, например, квартира, частный дом и прочие помещения, где будет находится

электронное техническое устройство, с помощью которого и совершено такого рода преступление.

Время совершения преступления является временным промежутком, в течение которого совершается или может быть совершено преступление. Существует утреннее, дневное, вечернее и ночное время совершения деяния. Однако каких-либо предпочтений во времени у таких преступлений нет – почти всегда время разное, за исключением только случая, когда они совершаются преступной группой, которая подбирает необходимое время исходя из работоспособности объекта посягательства.

Последним факультативным признаком выступает обстановка совершения преступления, представляющая собой совокупность объективных обстоятельств, при наличии которых осуществляется преступное деяние. Например, нарушение функционирования объекта критической инфраструктуры, при котором получить доступ к нему преступниками будет осуществлен намного проще и т.п.

Объективная сторона преступлений в сфере компьютерной информации обычно выражается в действии, хотя преступление, предусмотренное ст. 274 УК, может быть совершено как путем действия, так и путем бездействия. Составы преступлений, предусмотренных ст. 272 и 274 УК РФ сконструированы по типу формальных, а ч. 1 ст. 273 УК — по типу материального.

В соответствии с ч.1 ст. 272 УК РФ лицо подлежит уголовной ответственности за осуществление неправомерного доступа к компьютерной информации, если такое деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации.

В соответствии с Федеральным законом от 27.07.2006 №149 «Об информации, информационных технологиях и о защите информации» информация представляет собой сведения или данные, вне зависимости от формы их фиксации и передачи. Соответственно, компьютерная информация, являющаяся одним из видов информации, выражается в виде сведений,

находящихся в цифровом виде на компьютере, информационной сети, системе и прочих предназначенных для этого устройствах.

Под неправомерным доступом к компьютерной информации понимается получение несанкционированного доступа к информации, которая не является публично доступной путем совершения различных действий, выраженных в проникновении в компьютерную систему с возможным использованием специальных технических или программных средств, незащищенностью такой информации, посредством социальной инженерии и т.п.

Неправомерным признается также доступ к компьютерной информации лицом, не обладающим правом на получение и работу с данной информацией либо компьютерной системой, в отношении которых приняты специальные меры защиты, ограничивающие круг лиц, имеющих к ней доступ.

Соответственно, объективная сторона преступления, предусмотренного статьей 272 УК РФ, выражена в действии, направленном на получение доступа к компьютерной информации, ее уничтожение, искажение, блокировка и копирование[1].

Из этого вытекает, что состав преступления носит материальный характер и предполагает обязательное наступление одного или нескольких указанных в статье последствий:

1. Уничтожение информации - приведение ее в невозможное для использования по назначению состояние или исчезновение такой информации с цифрового носителя;

2. Блокирование информации, которое выражается в закрытии доступа к ней, что приводит к невозможности ее использования;

[1] Боровиков, В. Б. Уголовное право. Особенная часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов; под редакцией В. Б. Боровикова. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 505 с. — (Высшее образование). — ISBN 978-5-534-17301-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536930 (дата обращения 24.03.2025).

3. Модификация информации – преобразование данных злоумышленником путем внесения изменений в различные программы, базы данных, включая видоизменение текстовой информации;

4. Копирование информации, которое заключается в создании дубликата информации и ее перенос на другой цифровой носитель.

Предметом выступает сама компьютерная информация, то есть, конкретные сведения, сообщения, данные, представленные в форме упорядоченных электрических сигналов, возможных для восприятия и понимания, независимо от средств их хранения.

В статье 272^1 УК РФ объективная сторона предусматривает - незаконные использование или передачу, сбор и хранение компьютерной информации, в основании которой лежат персональные данные, которая получена путем неправомерного доступа к средствам ее сбора, хранения или иного вмешательства в их функционирование либо иным незаконным путем.

Из положений данной статьи вытекает, что объективная сторона выражается в:

1. Использовании персональных данных, то есть совершение всевозможных манипуляций, обязательной частью которых является их практическое применение, конечно же, в своих корыстных целях;

2. Передачей персональных данных выступают действия, связанные распространением, продажей, размещением их на интернет-ресурсах, в общем доступе. Т.е. данное действие выражается в предоставлении за вознаграждение или без личной информации о человеке третьим лицам.

3. Сбор персональных данных, который представляет под собой несанкционированный целенаправленный процесс извлечения, анализа, обработки и систематизации получаемой информации, содержащей персональные данные.

4. Хранение персональных данных, подразумевающее под собой деятельность по систематическому и централизованному накоплению

сведений, имеющих в своем содержании сведения, составляющие персональные данные.

5. Получение неправомерного доступа – деятельность лица, не имеющего в соответствии с ФЗ № 152-ФЗ «О персональных данных»[1] полномочиями доступа к персональным данным и осуществляющееся без согласия законного обладателя компьютерной информации, содержащей персональные данные.

6. Вмешательство в функционирование предусматриваем целенаправленное воздействие на ресурсы и хранилища, содержащие сведения, составляющие персональные данные, с целью получения доступа к ним или ограничения такого доступа путем программного воздействия на их хранилище.

Термин «Уничтожение» предполагает полное прекращение существование информации. «Уничтожить» - Прекратить существование кого-, чего-л.; истребить[2]. При удалении законный владелец лишается права доступа к информации, но она может существовать в объективной реальности, за пределами компьютерного устройства собственника информации. Тем, самым полагаем, что она не уничтожается совсем, а лишь удаляется с компьютерного носителя собственника информации, или иного хранилища. Таким образом, полагаем, наряду с термином «уничтожение» использовать термин «удаление» и изложить ч. 1 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в следующей редакции:

Доступ к охраняемой компьютерной информации, если это деяние повлекло неправомерно удаление, уничтожение, блокирование, модификацию либо копирование компьютерной информации, - …» далее по тексту;

---

[1] О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ // СПС «Консультант плюс»/ URL: - https://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/ (дата обращения 01.05.2025).

[2] Ожегов С.И., Н.Ю. Шведова. Толковый словарь русского языка. – М.: Академия наук СССР, 1949. С. 398.

В данном преступном деянии появляется такой предмет, как «персональные данные». Согласно пункту 1 статьи 3 вышеупомянутого закона под персональными данными понимается любая информация, относящаяся прямо или косвенно к определенному или определяемому физическому лицу, то есть субъекту персональных данных.

К такой информации относятся: фамилия, имя, отчество, дата рождения, место рождения, документы, содержащие сведения о их владельце, например, паспортные данные, номер мобильного телефона, место работы и занимаемая должность; банковские данные, доход и прочие личные сведения, использование которых может повлечь негативные последствия для их законного обладателя. Следует отметить, что номер телефона лица и его электронная почта являются персональными данными только в том случае, если они относятся к физическому лицу.

Статья 273 УК РФ устанавливает уголовную ответственность за создание, использование и распространение вредоносных компьютерных программ[1].

Объективную сторону составляет факт создания компьютерных программ либо иного компьютерного программного обеспечения, изначально предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или уничтожения средств защиты. Наиболее распространенными видами вредоносных программ являются компьютерные вирусы по типу трояна, черви, программы-шпионы, программы-вымогатели, логические бомбы и тому подобное. В основе объективной стороны данного преступления лежит:

1. Создание – целенаправленная деятельность злоумышленника, направленная на разработку и воплощение в действительность таких программ, использование которых причиняет неоспоримый вред лицу, на устройствах которого она появилась. Вред может касаться самого

[1] Приговор Фрунзенского районного суда г. Владимира №1-199/2024 от 23.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/rUi0IOY5QI5J/ (дата обращения 24.024.2025)

электронного устройства (ограничение в его использовании, блокировка, использование его ресурсов), так и информации, содержащейся на нем (уничтожение, блокировка, модификация, блокирование).

2. Распространение — это процесс перемещения вредоносной программы от одного ее держателя к другому различными способами, передача таких программ широкому и неопределенному кругу лиц. Самым распространенным способом распространения таких программ является социальная инженерия.

3. Использование – практическое применение вредоносных компьютерных программ в своих корыстных целях, в т.ч. для завладения компьютерной информацией, содержащейся на ПК, на котором оказалась данная программа. В зависимости от ее типа цели варьируются, однако остается неизменным факт корысти – перепродажа сведений другим преступникам, выкуп за разблокировку данных, извлечение выгоды их полученных сведений.

Само определение компьютерной программы вытекает из положения статьи 1261 ГК РФ[1]. (Программа представляет совокупность данных и команд, предназначенных для функционирования ЭВМ и других компьютерных устройств для достижения определенного результата).

Общественная опасность будет состоять в том, что вредоносные программы способны нарушить целость не только компьютерной информации и равно ее безопасность, но и нарушить функциональность самого ПК. В связи с этим, данный состав преступления необходимо считать формальным, т.е. не требуется наступления последствий.

В настоящий момент активно обсуждается проблема искусственного интеллекта при совершении преступлений. Так, на рассмотрение в Государственной Думе Российской Федерации находится проект

[1] Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 22.07.2024) // СПС «Консультант плюс». - URL:https://www.consultant.ru/document/cons_doc_LAW_64629/ce1359ed5b9bd99896d7a496c7887e7c223a2cbc/ (дата обращения 10.05.2025)

Федерального закона «О внесении изменения в статью 63 Уголовного кодекса Российской Федерации», основной целью которого выступает повышение ответственности за преступления, совершаемые с применением технологий искусственного интеллекта, а также для защиты граждан от цифрового мошенничества, которое становится одной из наиболее актуальных угроз в современной цифровой среде.

Злоумышленники используют современные технологии и психологические манипуляции для дестабилизации ситуации в стране, подрыва доверия граждан к государственным институтам и финансовым системам.

Соответственно, предлагается установить использование искусственного интеллекта в преступных целях в качестве отягчающего обстоятельства при совершении преступлений, предусмотренных УК РФ. Это позволит ужесточить наказание за преступления, совершенные с применением высоких технологий, и создать дополнительные правовые механизмы для защиты граждан.

Уголовная ответственность по статье 274 УК РФ наступает за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей[1].

Объективная сторона данного преступления состоит в действиях, приводящих к нарушению правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшем уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Предусмотренный комментируемой статьей состав преступления является материальным. Необходимым его элементом является причинение крупного ущерба. Понятие крупного ущерба законодателем

[1] Приговор Первомайского районного суда г. Новосибирска №1-436/2024 от 24.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/8HG5DkwEmsVJ/ (дата обращения 27.04.2025)

указано в примечании к ст. 272 УК[1]. Соответственно, сумма причиненного ущерба должна превышать один миллион рублей.

Объективную сторону преступления составляют действия, выражающиеся в трех основных формах:

1. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации. Смысл данного деяния состоит в том, что вышеуказанные действия совершаются с ошибкой и приводят к неблагоприятным последствиям как для компьютерной информации, так и для лица, совершившего ошибку.

2. Нарушение правил эксплуатации информационно-телекоммуникационных сетей и оконечного оборудования. В данном случае идет нарушение правил использование вышеуказанных систем, приводящее к уничтожению, копированию, блокировке или модификации содержащейся информации. Согласно ФЗ № 149 «Об информации, информационных технологиях и о защите информации» информационно-телекоммуникационная сеть представляет собой упорядоченную, технологически сложную систему, предназначенную для передачи по каналам связи информации, доступ к которой осуществляется с непосредственно с использованием вычислительной техники (тот же самый ПК, сетевые компьютеры в виде серверов и пр.). В силу такого сложного оборудования возникает необходимость упорядочения действия с ней, что выражается в совокупности принятых правил;

3. Нарушение правил доступа к информационно-телекоммуникационным сетям. Под доступом следует понимать реальную возможность воспользоваться сетями для конкретных действий. Соответственно, в силу нарушения установленных правил по вине

[1] Гладких, В. И. Уголовное право России в таблицах и комментариях. Общая часть: учебник для среднего профессионального образования / В. И. Гладких, М. Г. Решняк. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 212 с. — (Профессиональное образование). — ISBN 978-5-534-17477-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568689 (дата обращения 15.04.2025).

уполномоченного лица происходит уничтожение, копирование, блокировка модификация и другие последствия для содержащейся информации.

Норма является бланкетной, напрямую отсылает к определенным нормативным актам, инструкциям, регламентам и правилам, которые устанавливают порядок работы с информационно телекоммуникационными сетями и оконечным оборудованием в ведомстве или организации - например, Федеральный закон от 07 июля 2003 г. № 126-ФЗ «О связи»[1].

Состав данного преступления является материальным, т.к. должно последовать последствие в виде уничтожения, блокировки, модификации или копировании информации. Но, согласно диспозиции, такие действия должны причинить именно крупный ущерб – в данном случае на сумму свыше одного миллиона рублей.

Статьей 274[1] УК РФ установлена уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации.

Объективная сторона преступления, регламентированного ст. 274[1] УК РФ, выражена в создании, распространении и (или) использовании компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Понятие критической информационной инфраструктуры Российской Федерации отраженно в ФЗ от 26.07.2017 № 187-ФЗ[2]. Критическая

---

[1]О связи: Федеральный закон от 07.07.2003 N 126-ФЗ // СПС «Консультант плюс». - https://www.consultant.ru/document/cons_doc_LAW_43224/b819c620a8c698de35861ad4c9d9696ee0c3ee7a/

[2]О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_220885/

информационная инфраструктура представляет собой совокупность объектов критической информационной инфраструктуры, а также различные сети электросвязи, специально предназначенные для взаимодействия между ними.

Объект критической инфраструктуры выражен в виде различных информационных, телекоммуникационных и автоматизированных систем, предназначенных для управления критической информационной инфраструктурой. В силу своего колоссального значения возникла необходимость в защите данной сферы.

Помимо технической сферы, возникла также острая необходимость в защите критической инфраструктуры в виде должного закрепления о привлечении именно к уголовной ответственности за воздействие на нее в виде осуществления различных действий. Как раз таки они будут составлять объективную сторону. Перечень деяний представлен следующим образом:

1. Создание, распространении и (или) использование специальных программ и информационных ресурсов, целевым назначением которых будет являться осуществление неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации;

2. Осуществление неправомерного доступа к компьютерной информации, содержащейся в системе критической информационной инфраструктуры;

3. Нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи.

Кроме того, в ст. 274[1] УК РФ произошло объединение ранее рассмотренных деяний главы 28 УК РФ[1]:

1. Осуществление неправомерного доступа;
2. Использование специальных вредоносных программ;
3. Нарушение правил эксплуатации технических средств хранения, обработки или передачи компьютерной информации.

Для данного преступления характерно обязательное наступление последствий в виде причинения вреда. Соответственно, состав данного преступления будет являться материальным.

Статья 274[2] УК РФ определяет уголовную ответственность лицу, которое совершило 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.

Данная статья является относительно новой и «свежей» в сфере противодействия преступлениям в сфере компьютерной информации», отнесенная к главе 28 УК РФ – была введена Федеральным законом от 14.07.2022 № 260[2]. Введение ответственности за деяния, предусмотренные данной статьей обусловлены международной политической ситуаций в мире. По заявлениям представителей МИД Российской Федерации и высокопоставленных политических лиц наша страна по сей день находится в состоянии гибридной войны. Соответственно, атаки на наши

---

[1] Гладких В. И. Уголовное право. Особенная часть: преступления против общественной безопасности и общественного порядка: учебник для вузов / под общей редакцией Гладких В. И., Есаяна А. К. — Москва: Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-13708-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567546 (дата обращения 15.04.2025).

[2] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 N 260-ФЗ (последняя редакция) // СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/3d0cac60971a511280cbba229d9b6329c07731f7/

информационную сеть, ресурсы, операторов связи, русскоязычный сегмент сети «Интернет» возросли многократно именно по этой причине. В силу возросшей угрозы, операторы сотовой связи или как отражено в статье «связи общего пользования» обязан использовать специальный программно-аппаратный комплекс технических средств противодействия угрозам.

Такое средство противодействия угрозам устойчивости и безопасности приводит к снижению количества информационных угроз нашему государству путем ограничения доступа к запрещенной по решению суда на территории Российской Федерации информации. К ней относятся экстремистская информация, пропаганда культа самоубийств, фейковые новости о проведении Специальной Военной Операции, а также информации, дискредитирующей Вооруженные силы Российской Федерации, пропаганда наркотиков и подобных веществ и т.п. В случаях воздействия на такую систему происходят серьезные сбои в работе связи общего пользования, отключение отечественных Интернет-ресурсов или сбой в их стабильной работе.

Рассматриваемая статья по своей сути являются уникальной для главы 28 УК РФ в том аспекте, что в диспозиции обязательным условием является прямая ссылка на статью КоАП РФ, а именно 13.42[1]. Исходя из этого, к уголовной ответственности по статье 274[2] УК РФ будет привлекаться лицо, нарушившее порядок установки, эксплуатации и модернизации технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования сети «Интернет» (речь идет именно о русскоязычном сегменте) и сети связи общего пользования (интернет и IP телефония).

Объективную сторону рассматриваемого преступления будут составлять деяния, состоящие из:

---

[1] «Кодекс Российской Федерации об административных правонарушениях» от 30.12.2001 N 195-ФЗ (ред. от 07.04.2025) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_34661/01db86fb46c88f00ff06171e17bb7d66fcf09a53/ (дата обращения 10.05.2025)

1. Нарушения порядка установки, эксплуатации и модернизации технических средств противодействия угрозам устойчивости, безопасности и целостности.

2. Несоблюдения технических условий их установки или требований к сетям связи при использовании указанных технических средств. Смысл деяния заключается в отклонении от действующих норм и правил установки технических средств защиты, повлекшее нарушение их функционирование;

3. Нарушения требований к пропуску трафика. Его также называют сетевым трафиком. Он представлен в виде потока информации, попадающего в информационное поле нашей страны вместе со всем опасной информацией, которая была запрещена, и борьба, с которой возлагается на технические средства.

§ 2 Юридический анализ субъективных признаков составов преступлений, предусматривающих ответственность за преступления в сфере компьютерной информации

В теории уголовного права под субъектом преступления признается лицо, осуществляющее в том или ином виде запрещенное УК РФ негативно-правовое воздействие на охраняемый объект, и способное нести за это уголовную ответственность[1]. Признаки субъекта преступления образуют один из элементов состава преступления. Наличие у лица, совершившего преступление, определённых субъективных признаков может рассматриваться также как условие уголовной ответственности. Причем субъектом выступают граждане РФ, иностранные граждане, пребывающие на

[1] Бавсун, *М. В.* Квалификация преступлений по признакам субъективной стороны: учебник для вузов / М. В. Бавсун, С. В. Векленко. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2025. — 143 с. — (Высшее образование). — ISBN 978-5-534-18049-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/index.php/bcode/563066 (дата обращения 10.04.2025).

территории РФ, лица, имеющие двойное гражданство (т.н. бипатриды) и лица без гражданства вообще.

Важно учитывать, что под субъектом преступления понимается не отдельно взятое физическое лицо, а, прежде всего, совокупность признаков, которые определяют юридическое и психофизическое его состояние с правовой точки зрения, обязательных для привлечения человека к ответственности за преступление.

Близким по значению является понятие «личность преступника». Но данные понятия имеют разные объемы: личность является более широким, чем понятие субъект, т.к. включает не только юридическую составляющую. Личность рассматривается с точки зрения криминологии и учитывает особенности отдельно взятого лица, совершившего преступление. Необходимость учитывать личностную характеристику лица является обязательным условием для назначения и индивидуализации наказания, что также отражено в Общей части УК РФ. Прежде всего, это вытекает из основной цели уголовного законодательства РФ – исправление осужденного, а не его наказание. Именно поэтому субъект преступления рассматривается в качестве совокупности признаков.

Как и каждый элемент преступления, субъект обладает своими уникальными признаками, которые исходят из его определения. Согласно российскому законодательству к ним относятся:

1. Наличие в ходе деяния, запрещенного УК РФ под угрозой наказания, физического лица;
2. Достижение определенного возраста, определенного законодателем;
3. Установление вменяемости лица путем проведения соответствующих экспертиз и признания их судом.

Особенностью является тот факт, что само определение понятия «физическое лицо» в УК РФ не закреплено. Однако смысл представляется правоприменителям достаточно очевидным: в качестве физического лица в правоотношениях выступает только человек.

Как показала практика, существуют такие случаи, когда общественно опасное деяние совершает лицо, не обладающее вышеопределенными признаками субъекта преступления. Из этого вытекает, что такое лицо не может быть подвергнуто уголовному наказанию. Перейдем же к их рассмотрению.

Возраст уголовной ответственности — это такое количество прожитых лет, при достижении которых лицо может быть привлечено к уголовной ответственности за совершение общественно опасного деяния. Согласно УК РФ, возраст наступления уголовной ответственности закреплен в статье 20 – по общему правилу уголовная отнесенность за виновно совершенное деяние наступает с шестнадцати лет. Однако законодателем определено, что за определенные преступления наступает и с четырнадцати лет.

Законодатель установил такое разграничение вследствие того, что к уголовной ответственности с четырнадцати лет привлекают за преступления, обладающие повышенной опасностью. Кроме того, считается очевидным, что совершение таких деяний является преступным и, соответственно несовершеннолетние отчетливо понимают, что они совершают и что за их деянием последуют последствия.

В уголовном законодательстве большинства стран установлен минимальный возраст уголовной ответственности — некий предельный возраст, по достижении которого лицо считается способным осознавать социальную значимость всех охраняемых уголовным правом объектов.

Вопрос о выборе определенного минимального возраста уголовной ответственности является уголовно-политическим - в каждой стране и в конкретный исторический период он решается по-своему, исходя из политико-правовой и социально-экономической обстановки.

Так, в США в 33 штатах установлен минимальный возраст привлечения к уголовной ответственности по преступлениям федерального уровня – 11 лет,

во Франции – 13 лет, ФРГ – 14 лет, в Великобритании – от 10 до 17 лет (варьируется в зависимости от совершенного деяния)[1].

В связи с привлечением лица к ответственности возникает необходимость определения его возраста. В России, действует судебная практика, согласно которой лицо считается достигшим определенного возраста не в день рождения, а начиная со следующих суток, при этом учитываются часовые пояса места рождения лица и места совершения преступления; если возраст устанавливается судебно-медицинской экспертизой, днем рождения подсудимого считается последний день года, названного экспертами, а если назван минимальный и максимальный возможный возраст лица, суд исходит из минимального возраста.

Исходя из количества преступлений и лиц, их совершивших, на основе анализа научных работ и различных диссертаций на рассматриваемую тему, нами хотелось бы предложить понизить возраст уголовной ответственности лиц, совершающих преступления, предусмотренные главой 28 УК РФ. Однако, российское уголовное законодательство построено на принципах демократизации, либерализации и лояльного отношения к несовершеннолетним. В силу этого понижение возраста привлечения к ответственности по указанным статьям не приведет к желаемому, а самое главное, к правильному результату. Поэтому нами предлагается осуществлять перевоспитание путем не применения уголовно-правовых норм, а в рамках проведения работ по цифровой гигиене и вытекающей из нее работе по цифровому воспитанию, где будет рассказано не только о последствиях совершения того или иного деяния, но и как обезопасить себя от подобного рода цифровых преступлений.

---

[1] Крылова Н. Е. Уголовное право зарубежных стран. Общая часть: учебник для вузов / ответственный редактор Н. Е. Крылова. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 576 с. — (Высшее образование). — ISBN 978-5-534-18747-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/578970 (дата обращения 07.03.2025)

Следующим критерием привлечения лица к ответственности является его вменяемость. Вменяемость представляет собой это нормальное, стабильное психическое состояние лица, при котором оно способно понимать своё место в обществе и отдавать отчёт своим действиям.

Соответственно, невменяемость — противоположное состояние лица, при котором оно не осознает фактический характер и общественную опасность своих действий или бездействия, либо руководить ими вследствие хронического психического расстройства, временного психического расстройства, слабоумия либо иного болезненного состояния психики, о чем напрямую сказано в статье 21 УК РФ. Соответственно, если будет установлен факт невменяемости лица, то оно не будет подлежать ответственности.

Для рассматриваемых преступлений не характерно состояние невменяемости, что является особенностей такого разновидности преступных деяний.

Рассмотрим же теперь второй субъективный признак преступления.

Субъективная сторона преступления выражается во внутреннем психическом отношении лица к совершаемому им общественно опасному деянию.

В отличие от признаков объективной стороны, которая внешне выражена и доступна для восприятия окружающими, признаки субъективной стороны по своей сути скрыты от других, и будут определены на основании показаний, данных лицом, совершившим то или иное уголовно наказуемое деяние, а также путем анализа и реальной оценки объективных признаков преступления.

Наиболее распространенным в современных научных и учебных изданиях является представление о субъективной стороне преступления как о совокупности признаков, характеризирующих именно психическую сторону деяния, включающую в себя вину, мотив и цель.

Известный российский ученый-правовед, доктор юридических наук, профессор, автор учебных изданий по уголовному праву Алексей Иванович

Рарог[1] определил субъективную сторону так, что под ней понимается активная психическая деятельность лица, непосредственно связанная с совершением преступного деяния.

Вина характеризуется следующими обязательными элементами:

- Интеллектуальный — это фактическая способность лица осознавать сложившуюся ситуацию, в которой он оказался, последствия своего поведения и их общественную опасность. Соответственно, рассматривая преступления, предусмотренные главой 28 УК РФ, интеллектуальный момент наступает, когда лицо понимает, что своими получает доступ к той компьютерной информации или совершает иное деяние, предусмотренное данной и какие вследствие этого наступают последствия.
- Волевой выражается в осознанном направлении своих умственных и физических сил на принятие итогового решения, достижения ранее обозначенной цели, выбор определенного варианта своего поведения. Таким образом, лицо направляет все свои возможности на достижение преступного результата, чем, в данном случае, является получение доступа к компьютерной информации.

Форма вины представляет собой непосредственное сочетание как интеллектуальных, так и волевых признаков, свидетельствующих о непосредственном отношении лица к совершаемому им деянию и соответствующим последствиям.

Согласно российскому уголовному законодательству вина подразделяется на две основные формы – умысел и неосторожность.

Умысел представляет собой связь осознания лицом сущности совершаемого им противоправного деяния, предвидения его последствий и наличия воли, направленной к его совершению. По своей сути большинство

[1]Рарог А.И. Общая часть учебник издание второе переработанное и дополненное. Под редакцией доктора юридических наук, профессора, Рарога А.И, профессора Чучаева А.И. // Образовательная платформа ALL Адвокатура [сайт]. с. 558 URL: https://all-advokatura.ru/upload/iblock/c21/c2111d8ca95fddb9f46da5ea203966b7.pdf (дата обращения 05.05.2025)

преступлений совершаются умышленно –порядка 90% всех преступлений, причем не только в нашем государстве, но и за рубежом.

В силу различия интеллектуального аспекта умысла, выделяют два основных его проявления:

- Прямой умысел;
- Косвенный умысел.

При прямом умысле лицо однозначно осознает общественную опасность своего деяния в виде действия или бездействия, предвидит реальную возможность или неизбежность наступления общественно опасных последствий (т.н. интеллектуальный момент) и непосредственно желает их наступления (волевой момент).

При косвенном умысле виновный осознает не закономерную неизбежность последствий, а лишь реальную возможность их наступления. С точки зрения волевого элемента виновный прямо не желает, но сознательно допускает их наступление или относится к ним без должного внимания.

Неосторожность же характеризуется легкомысленным расчётом на предотвращение наступления опасных последствий либо отсутствием предвидения наступления таких последствий. Неосторожность встречается гораздо реже, чем умысел, однако по своим последствиям неосторожные преступления могут быть ничуть не менее опасными, чем умышленные. Неосторожность при этом может быть двух видов: преступное легкомыслие и преступная небрежность.

- При преступном легкомыслии виновный предвидит возможность наступления опасных последствий (интеллектуальный момент), не желает их, но без каких-либо достаточных оснований самонадеянно рассчитывает на их предотвращение (волевой момент). При этом лицо не видит в своих действия общественную опасность, хотя и осознаёт, что они нарушают определённые правила предосторожности.
- При преступной небрежности виновный уже не предвидит возможность наступления общественно опасных последствий, хотя, по своей

сути, должен был и мог их предвидеть. Лицо может быть привлечено к ответственности за такие действия, поскольку его поступки связаны с пренебрежительными отношениями к закону, требованиям безопасности и интересам других лиц.

По своей сути, уголовно-правовое значение мотивов и целей представляется ровно таким же, как и любых других факультативных признаков. Они могут выступать, в первую очередь, в роли составообразующего, когда они непосредственно включены в конструкцию состава преступления, а также могут признаваться квалифицирующими признаками, будь то отягчающими или смягчающими уголовную ответственность обстоятельствами.

Итак, мотивом преступления принято считать вызванные существующими потребностями лица факторы, которые обуславливают выбор лицом не только преступного варианта поведения, но и конкретную линию его поведения. Мотив напрямую связан с целью такого поведения лица.

Целью преступления выступает возведенное в идеал представление лица о конечном результате своего преступного деяния, которого оно стремится достичь всеми своими действиями. В самом начале цель преступления формируется на глубинном подсознательном уровне, а в дальнейшем переходит в осознанное влечение к удовлетворению потребности, составляющей мотив преступления.

Цель и мотив выступают психологической основой для формирования у субъекта отношения к совершаемому деянию. Мотивы и цели в умышленных преступлениях носят исключительно преступный характер, так как цели, которых желает достичь лицо, связаны с причинением вреда охраняемым законом общественным отношениям.

А вот в неосторожных преступлениях мотивы, как и цели, носят скорее нейтральный характер потому не могут быть признаны преступными.

Мотивы преступлений в сфере компьютерной информации, которые предусмотрены главой 28 Уголовного кодекса РФ выглядят следующим образом:

- Корыстная заинтересованность. Спрос на незаконно полученную конфиденциальную информацию значителен, и преступники стремятся получить материальную выгоду за свое деяние;
- «Интеллектуальный вызов». Стремление продемонстрировать собственный профессионализм, а также проявить себя перед другими киберпреступниками также может быть мотивом компьютерных преступлений;
- Личная неприязнь. Она может послужить поводом для незаконного доступа к компьютерной информации, её уничтожения, блокирования, модификации либо копирования.
- Прочие мотивы, исходящие из особенностей деяния лица.

Помимо этого, эмоциональную составляющую также принято относить к субъективной стороне преступного деяния. Уголовно-правовое значение имеет только состояние чрезвычайно сильного кратковременного, высоко интенсивного эмоционального возбуждения, бурно протекающего и характеризующегося своей внезапностью возникновения, кратковременностью протекания, значительным характером изменений сознания, нарушением волевого контроля за действиями —аффект.

Аффект может быть физиологическим и патологическим. При физиологическом аффекте возникшее состояние представляет собой интенсивную эмоцию, которая доминирует в сознании человека, снижает его контроль за своими поступками, характеризуется сужением сознания, определенным торможением интеллектуальной деятельности. Патологический аффект характеризуется полным помрачением сознания и неуправляемым импульсивным действием. Он является обстоятельством, исключающим вменяемость.

Особенность рассматриваемых преступлений в сфере компьютерной информации заключается в том, что мотивы и цели преступлений в сфере не являются обязательными признаками субъективной стороны и, следовательно, на квалификацию повлиять не могут. Однако установление мотивов и целей все же должны производиться, соответственно, учитываться при назначении наказания. А наличие аффекта для рассматриваемых преступлений вообще не характерно.

Итак, субъектом преступлений, предусмотренного Главой 28 УК РФ является вменяемое физическое лицо, достигшее к моменту совершения преступного деяния возраста 16 лет.

По своей сути деяния, предусмотренные 28 УК РФ является умышленными и могут быть совершенны 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. Мотивы могут весьма разниться – от корыстного, за предоставление другим лицам компьютерной информации, или же будет хулиганский, выражающийся в желании преступника продемонстрировать свои навыки и способности третьим лицам. Цель же деяния отражена в диспозиции данной статьи.

Для статей 272^1 ,274, 274^2 будет характерно наличие специального субъекта. Специальный субъект преступления — это такое лицо, которое, обладающее помимо общих признаков субъекта дополнительными, необходимыми для привлечения его к уголовной ответственности за конкретное совершённое преступление[1]. В данном случае, в силу своего должностного положения, лицо, используя его, причиняет вред иным лицам,

[1] Диканова Т. А., Ображиев К. В. Уголовное право России. Особенная часть. Том 2. М.: Юрайт. 2023. 640 с. Текст: электронный // URL: https://search.rsl.ru/ru/record/01010335420 (дата обращения 18.04.2025)

обществу и государству в целом, что необходимо расценивать как отягчающее обстоятельство. Т.е. данное положение дополняет основную часть субъекта – 16-летний возраст и вменяемость. Это было необходимо для того, чтобы дисциплинировать деятельность должностных лиц с помощью уголовного закона.

Особенность мотивов статьи 274^1 заключается в том, что ко всем остальным ранее рассмотренным добавится еще политический – совершение атаки на государственные структуры в силу негативного отношения к действующей власти в РФ, так еще и этот мотив будет тесно переплетен с корыстным в виде желания получить вознаграждение от враждебно настроенных по отношению к РФ лиц, за чей счет и будет произведена кибератака.

§ 3 Квалифицированные и особо-квалифицированные признаки составов преступлений в сфере компьютерной составов преступлений в сфере компьютерной информации

Рассмотрев основной состав преступлений, предусмотренных главой 28 УК РФ, перейдем к квалифицированным и особо квалифицированным признакам обозначенных ранее деяний.

Состав преступления играет особо важную роль в квалификации преступлений: из общей массы признаков конкретного деяния выделяются признаки состава преступления, которые, в свою очередь ставятся в соответствие юридическим признакам, закреплённым в диспозиции уголовно-правовой нормы.

Квалифицированные признаки преступления представляют собой свойство преступного деяния, характеризующие его повышенной по сравнению с основным составом общественной опасностью.

Например, к таким признакам относятся:

- Совершение преступления группой лиц;
- Повышенная тяжесть последствий;
- Способ совершения деяния;
- Какие-либо социально значимые составляющие личности преступника или же самого потерпевшего.

Квалифицированные признаки выступают средством дифференциации и индивидуализации уголовной ответственности, что, соответственно, выражается в новых пределах наказуемости за преступление.

Особо же квалифицированные признаки формируют состав преступления, при котором наряду с основными признаками имеются особо отягчающие обстоятельства, увеличивающие общественную опасность по сравнению с квалифицированным составом преступления.

Федеральным законом № 420 от 07.12.2011[1] статья 272 УК РФ была дополнена ч. 2 и квалифицирующими признаками - совершение предусмотренного того же преступного деяния, которое причинило крупный ущерб или было совершено из корыстных мотивов.

Согласно нижеприведенному примечанию, крупный ущерб составляет причинение ущерба на сумму, превышающую один миллион рублей. Причем, данное примечание относится ко всем статьям главы 28 УК РФ.

Корыстная заинтересованность затрагивает мотив виновного лица и означает желание получить доход, прибыль или какую-либо материальную выгоду в виде вознаграждения за совершенное преступное деяние.

---

[1] О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации: Федеральный закон от 07.12.2011 N 420-ФЗ // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_122864/

Совершение деяния группой лиц (т.е. двумя и более лицами) по предварительному сговору (заранее договорившись о совершении преступления) или организованной группой (структурированной группой или объединением нескольких групп, действующих под единым руководством) лицом при использовании своего служебного положения, уже само по себе отягчает деяние. Именно об этом и сказано в ч.3 статьи 272 УК РФ и, соответственно, считается особо квалифицированными признаками данного преступления.

Однако для того, чтобы признали содеянное совершенное группой лиц или предварительному сговору необходимо установить, что все субъекты полностью или частично выполняли действия, предусмотренные диспозицией. Т. е. преступники обеспечивали неправомерный доступ к информации, или уничтожали, или модифицировали, или блокировали, или копировали информацию. Причем действия участников организованной группы будут квалифицироваться по ч. 3 ст. 272 УК РФ вне зависимости наличия объективной стороны[1].

Использование служебного положения означает, что лицо осуществляет доступ к компьютерной информации, незаконно используя права, предоставленные ему исключительно в силу выполняемой им служебной деятельности. При этом виновное лицо использует предоставленные ему по службе права вопреки законным интересам человека, общества или государства в целом.

Частью 4 обозначено, что действия, которые также предусмотрены предыдущими частями, повлекли тяжкие последствия. Разъяснение и определение таких последствий последовало в Постановлении Пленума Верховного Суда Российской Федерации от 15.12.2022 № 37[2]. Итак, в

---

[1] Приговор Октябрьского районного суда г. Иваново № 1-308/2024 от 28.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/sr7cmrYRke1V/ (дата обращения 22.04.2025)

[2] Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 "О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной

преступлениях 272 - 274[1] УК РФ под тяжкими последствиями следует понимать остановку на длительное время или нарушение нормального функционирования предприятия, учреждения или организации, получение доступа к информации, являющейся тайной и охраняемой законом и т.п.

В части 2 статьи 272[1] УК РФ указано, что, если деяния совершены в отношении компьютерной информации, включающей в себя персональные данные несовершеннолетних, иные специальные категории персональных данных или биометрические персональные данные влекут более суровую уголовную ответственность, что также является квалифицирующим признаками преступления.

Часть 3 содержит ряд отягчающих, ранее рассмотренных, признаков деяния:

- Корыстная заинтересованность;
- Причинение крупного ущерба;
- Совершение группой лиц по предварительному сговору;
- Использование лицом своего служебного положения

Частью 4 предусмотрена ответственность за трансграничную передачу персональных данных. Такая передача означает вывоз носителя с персональными данными за границу РФ, а также на территории иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Преступление признается совершенным организованной группой, если оно совершено объединением с преступным умыслом лиц, объединившихся заранее для совершения данного преступлений

Часть 2 статьи 273 УК РФ предусматривает повышенную уголовную ответственность за деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или

информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_434573/

совершенные из корыстной заинтересованности. Содержание этих квалифицирующих признаков соответствует содержанию аналогичных признаков ранее рассмотренных составов преступлений[1].

Часть 3 данной статьи предусматривает повышенную уголовную ответственность за деяния, повлекшие тяжкие последствия или создали угрозу таких последствий. Процесс создания специализированных вредоносных программ может быть осуществлен только подготовленными, имеющими соответствующее образование лицами, которые в силу своей профессиональной подготовки осознают их целевое предназначение и, соответственно, последствия использования таких программ.

Часть 2 статьи 274 УК РФ в качестве квалифицирующего признака также устанавливает более тяжелую уголовную ответственность за деяние, если оно повлекло тяжкие последствия или создали угрозу их наступления. Что также было предусмотрено ранее рассмотренными преступлениями.

Часть 4 274^1 УК РФ предусматривает следующие квалифицирующие признаки:

- Совершение деяния группой лиц по предварительному сговору или организованной группой;
- Совершение деяния лицом с использованием своего служебного положения.

Часть 5 статьи предусматривает такой квалифицирующий признак, как тяжкие последствия, имеющие значение для безопасности критической информационной инфраструктуры. Критерии тяжести последействий были предусмотрены Постановлением Пленума Верховного суда № 37 от 15.12.2022 года.

---

[1] Бастрыкин А. И. Уголовное право. Особенная часть: учебник для вузов / под общей редакцией А. И. Бастрыкина; под научной редакцией А. И. Чучаева. — Москва: Издательство Юрайт, 2025. — 468 с. — (Высшее образование). — ISBN 978-5-534-12079-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580312. (дата обращения 21.04.2025).

Частью 274^2 УК РФ предусмотрены тяжкие последствия для устойчивости функционирования сети связи общего пользования. Например, массовые сбои, создающие угрозу общественной безопасности, а также использование служебного положения[1].

Уголовная ответственность по статье 274^2 УК РФ наступает, когда общественная опасность деяния существенно выше и наступают или могут наступить серьёзные последствия. Например, реальная дестабилизация сети или создание угрозы безопасности. При этом в научной среде отмечается сложность применения статьи из-за широких формулировок («угрозы устойчивости», «целостности функционирования» и т. п.) и отсутствия достаточной судебной практики.

ГЛАВА 3 ПРОБЛЕМЫ КВАЛИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ

§ 1. Квалификация преступлений в сфере компьютерной информации, совершенных в соучастии

В уголовном праве под соучастием принято понимать умышленное совместное участие двух или более лиц в совершении умышленного преступления.

Институт соучастия вызывает большое число споров в уголовно-правовой науке, является венцом общего учения о преступлении и считается труднейшим разделом уголовного права.

По общепринятому и общемировому правилу соучастие принято считать более опасной формой преступной деятельности, чем совершение того же деяния,

---

[1] Сверчков В. В. Уголовное право. Особенная часть: учебник для среднего профессионального образования / В. В. Сверчков. — 12-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 421 с. — (Профессиональное образование). — ISBN 978-5-534-20225-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557823 (дата обращения12.05.2025)

но единолично. Учеными-правоведами это обосновано тем, соучастие представляет собой такое объединение усилий, которое придаёт их деятельности новое качество с вытекающими, более тяжкими последствиями, т.к. наносится более серьезный ущерб охраняемым законом общественным отношениям[1].

По своей сути при соучастии ключевое значение играет совместность деятельности нескольких лиц, интересы и силы которых направлены на выполнение общего, конкретного и единого для всех преступления. Совместность выражается в качестве объединения усилий виновных по совершению преступления, и достижение ими единого преступного результата. Кроме того, такой результат, который находится в причинной связи с действиями всех соучастников.

В основном, соучастие осуществляется путем совершения активных действий лиц, но бывают случаи, когда соучастие совершается путем бездействия.

Исходя из описания в литературе, для совместного совершения преступного деяния будут характерны следующие признаки:

- Предварительная договоренность их объединения для совершения преступления;
- Высокий уровень организованности, направленный на разработку, планирование, подготовку, поиск средств и орудий, разбитие на роли и конечное совершения преступлений;
- Высокая степень устойчивости, выраженная в стабильном, строгом и определенном составе участников объединения, тесная взаимосвязь между ними, согласованность действий участников, направленных на достижение преступного

[1] Савельев Д. В. Соучастие в преступлении. Преступная группа: учебник для вузов / Д. В. Савельев. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 134 с. — (Высшее образование). — ISBN 978-5-534-17840-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/565269. (дата обращения 27.04.2025)

Повышенная опасность совместного совершения рассматриваемых преступлений при различных групповых формах соучастия отражается в квалифицированных и особо квалифицированных признаках составах этих преступлений. Признаки совершения преступления группой лиц по предварительному сговору и организованной группой являются квалифицирующими преступления, ответственность за которые предусмотрена практически во всех статьях Главы 28 УК РФ. О предварительном сговоре, организованной группе и преступной организации сказано в статье 35 УК РФ.

Следует отметить, что фактическое установление всех участников совершения рассматриваемых преступлений весьма тяжело, в силу использование ими различной компьютерной техники, различных программ, скрывающих их, а также возможного весьма удаленного нахождения.

Итак, преступление признается совершенным по предварительному сговору только в том случае, когда лица заранее договорились о совместном совершении именно этого преступления.

Что касается организованной группы, то в данном случае речь идет о совершение преступления устойчивой группой лиц, которые объединились заранее для совершения одного или нескольких преступлений. В данном случае речь идет о предварительной договоренности, т.е. до начала совершения самого преступного деяния. В данном случае также будет характерен лидер, «во благо» преступного умысла которого будут работать другие.

Наибольшую опасность представляет преступное сообщество. Под которым понимается структурированная организованная группа или объединение таких групп, которые действуют под централизованным руководством, члены которых объединены в целях совместного совершения одного или нескольких тяжких либо особо тяжких преступлений для получения прямо или косвенно финансовой или иной материальной выгоды. В рассматриваемых деяниях такое сообщество представлено в виде

преступной хакерской организацией, носящий транснациональный характер, которую, в первую очередь, интересует лишь корыстный мотив[1].

В групповых преступлениях умыслом каждого из соучастников должны охватываться определенные в диспозиции статей действия и вытекающие из них последствия в виде уничтожения, блокирования, модификации, копирования информации (в отдельных случаях содержащей персональные данные) или возможность причинение вреда охраняемой законом информации, критической информационной инфраструктуре Российской Федерации либо осознанность или понимание предназначенности созданных вредоносных программ.

§ 2. Квалификация неоконченной преступной деятельности при совершении преступлений в сфере компьютерной информации

Неоконченное преступление представляет собой виновно совершенное общественно опасное деяние в виде действия или бездействия, запрещенное УК РФ, но которое не содержит всех признаков преступления, и которое, и не было доведено до конца по причинам, не зависящим от самого виновного.

Неоконченное преступление отражено в статье 29 УК РФ и таковым признается приготовление к преступлению и покушение на само преступление.

Приготовление к преступлению обозначает поиск, изготовление, приспособление различных средств и орудий, которые будут использованы для совершения преступления или уже в момент совершения такого преступления. Помимо этого, к приготовлению будет относится и поиск соучастников, их

[1] Сверчков В. В. Уголовное право. Общая часть. Учебно-методический комплекс: учебник для вузов / В. В. Сверчков. — Москва: Издательство Юрайт, 2025. — 649 с. — (Высшее образование). — ISBN 978-5-534-11726-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566527. (дата обращения 08.05.2025)

организация или какое-либо иное умышленное создание благоприятных условий для совершения преступного деяния. Но во всех вышеперечисленных случаях обязательно, чтобы такое деяние не было доведено до своего логического конца по обстоятельствам, не зависящим от преступника. Уголовно наказуемым приготовление признается только в случаях, когда такого рода подготовка осуществляется к тяжким и особо тяжким преступлениям.

Под покушением на преступление понимается умышленное совершение активных действий или же пассивное бездействие, которое направлено на совершение самого преступления, однако оно не доведено до конца также по не зависящим обстоятельствам от виновного.

Рассматриваемые преступления, а именно, ч. 1 ст. 272, ч. 1 ст. 274, относятся к категории небольшой тяжести, и, соответственно, максимальное наказание за их совершение не превышает двух лет лишения свободы. Деяние, предусмотренное ч. 1 ст. 273, признается преступлением средней тяжести, поскольку максимальный срок наказания в виде лишения свободы не превышает четырех лет лишения свободы[1]. Отсюда вытекает, что за приготовление к данным преступлениям не будут подвергаться уголовному наказанию.

Постановление Пленума № 37 дает четкое определение, когда деяние, предусмотренное статьей 272 УК РФ, необходимо признать покушением на такое преступление. Если лицо, намереваясь осуществить уничтожение, блокирование, модификацию или копирование охраняемой законом компьютерной информации, выполнило все действия, необходимые для неправомерного доступа к компьютерной информации, либо осуществило такой доступ, однако ни одно из последствий, предусмотренных частью 1 статьи 272 УК РФ, не наступило по независящим от него обстоятельствам (например, в результате срабатывания автоматизированных средств защиты информации или

[1] Капинус О. С. Уголовное право России. Особенная часть: учебник для вузов — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 1189 с. — (Высшее образование). — ISBN 978-5-534-18351-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/534839 (дата обращения 23.04.2025)

действий лиц, осуществляющих ее защиту), такие действия следует квалифицировать как покушение на совершение данного преступления.

Чтобы считать преступное деяние, отраженное в статье 273 УК РФ в качестве оконченного, достаточно будет установление факта создания элемента кода вредоносной компьютерной программы, с помощью которой осуществляется неправомерный доступ к компьютерной информации. Однако, если по независящим от лица обстоятельствам будет исключена возможность реального применения или использования на различных этапах создания программы, то деяние следует квалифицировать как покушение на преступление.

Создание или использование лицом вредоносной компьютерной программы либо иной компьютерной информации подобного рода для неправомерного доступа к охраняемой законом компьютерной информации образует изготовление им средства совершения или создание условий для совершения преступления, т.е. приготовительную преступную деятельность. В таких случаях приготовление к преступлению полностью совпадает с составом преступления, предусмотренным ст. 273 УК РФ, и перечисленные действия лица при их полном окончании необходимо квалифицировать по совокупности преступлений, ответственность за которые предусмотрена соответствующими частями ст. 272 и 273 УК РФ. Иными словами, каждая последующая стадия совершения преступления поглощает все предыдущие, и они не требуют самостоятельной уголовно-правовой оценки[1].

Так, ч. 2 ст. 274[1] УК РФ регламентирует ответственность за совершения таких действий в качестве единого преступления – учтенной законодателем совокупности преступлений. Поэтому при осуществлении неправомерного доступа к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре РФ, с использованием

[1] Козаченко И. Я. Уголовное право. Особенная часть. Краткий курс: учебник для вузов / ответственный редактор И. Я. Козаченко. — Москва: Издательство Юрайт, 2025. — 263 с. — (Высшее образование). — ISBN 978-5-534-18051-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560123 (дата обращения 09.04.2025)

вредоносных программ, повлекшее причинение вреда такой инфраструктуре, квалифицируется только по ч. 2 ст. 274^1 УК РФ.

Таким образом, если приготовление или покушение на какое-то преступление полностью совпадает с другим составом преступления против безопасности компьютерной информации, такие действия квалифицируются по совокупности преступлений, за исключением случая наличия законодательно учтенной совокупности преступлений. В качестве покушения на преступление можно отнести деяние лица, которому по независящим обстоятельствам не удалось довести свою преступную деятельность до конца.

В соответствии с правилами, выработанными в теории квалификации преступлений, такое деяние подлежит квалификации в качестве оконченного преступления и полностью исключает уголовно-правовую оценку как покушение на действие, выполненного частично. Некоторое значение могут иметь вопросы толкования некоторых объективных признаков составов преступлений против безопасности компьютерной информации для квалификации их неоконченными. Так, отдельно необходимо рассмотреть признак получения лицом «доступа», наличествующего в ст. 272 УК РФ.

Доступ к компьютерной информации может выражаться в получении лицом права на чтение (ознакомление) компьютерной информации, которое не является уголовно-наказуемым последствием. После ознакомления с компьютерной информацией у лица может возникнуть умысел на осуществление уголовно-наказуемых действий в виде удаления, блокирования, модификации, копирования. Между действием в виде ознакомления и другими действиями может иметься значительный временной промежуток, который также может связываться тем, что лицо не в состоянии получить права на иные виды доступа к компьютерной информации. Поэтому установленный прямой умысел лица на уголовно-наказуемые деяния в виде удаления, блокирования, модификации либо копирования компьютерной информации, непосредственно направленные на такую деятельность, прерванный по независящим от этого лица обстоятельствам, следует квалифицировать как

покушение на преступление. Соответственно, без наступления последствий не образуется состава преступления. Однако осуществляется причинение ущерба конституционным правам человека, где строго закреплено право на неприкосновенность частной жизни. В конечном итоге этот вопрос до сих пор остается весьма спорным.

Кроме того, если действия, отраженные в Главе 28 УК РФ[1], выступали как способ совершения иных преступлений, то в данном случае лицо подлежит ответственности уже по совокупности преступлений. Например, если мошенничество в сфере компьютерной информации совершено посредством осуществления неправомерного доступа к компьютерной информации или с использованием вредоносных компьютерных программ, то необходима дополнительная квалификация по статье 272 или 273 соответственно.

§ 3. Квалификация преступлений против безопасности компьютерной информации при их множественности

Множественность преступлений выражается в виде совершения одним лицом двух и более преступных, уголовно наказуемых деяний, каждое из которых является самостоятельным преступлением и за которое следует наступление соответствующей санкции, предусмотренной в УК РФ. Согласно российскому законодательству, выделяют два основных вида множественности – совокупность и рецидив.

[1] Наумов А. В., Кибальник А. Г. Преступления против общественной безопасности и общественного порядка: учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — Москва: Юрайт, 2025. — 158 с. — (Высшее образование). — ISBN 978-5-534-18589-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. с. 158 — URL: https://urait.ru/bcode/563347/p.158 (дата обращения: 01.05.2025).

Совокупность преступлений подразумевает под собой совершение лицом двух или более преступлений, ни за одно из которых лицо в конечном счете еще не было осуждено Совокупностью преступлений также следует признать и одно действие (бездействие), содержащее признаки преступлений, предусмотренных двумя или более статьями.

Если преступление предусмотрено как общей, так и специальной нормой, то совокупности в данном случае не будет, а ответственность наступит по специальной норме. Совокупность преступлений бывает двух ключевых видов: реальная и идеальная.

Реальная совокупность преступлений представляет собой совершение двух или более самостоятельных преступных деяний, при условии, что ни за одно из них лицо не было осуждено. Число фактических деяний при этом должно соответствовать числу преступлений: два деяния — два преступления и т.д. Эта форма множественности наиболее часто встречается в практической деятельности[1].

Реальную совокупность могут составлять как однородные, так и разнородные, а также и тождественные преступления.

За идеальную совокупность следует принимать такое действие (бездействие), содержащее именно признаки двух и более составов преступлений. Однако, идеальная совокупность может состоять как из двух, так и трёх и более преступных деяний.

Рецидив же представляет собой совершение умышленного преступного деяния лицом, уже имеющим судимость, если она не снята и не погашена в установленном законом порядке за ранее совершённое умышленное преступление. Как правило, рецидив влечёт за собой усиление уголовной ответственности[2].

---

[1] Савельев Д. В. Уголовное право. Общая часть: учебник для вузов / Д. В. Савельев. — Москва: Издательство Юрайт, 2025. — 374 с. — (Высшее образование). — ISBN 978-5-534-21540-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/575502 (дата обращения 06.05.2025)

[2] Наумов А. В., Кибальник А. Г. Уголовное право. Общая часть: учебник для вузов / ответственные редакторы. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 448 с. — (Высшее образование). — ISBN 978-5-534-18585-0. — Текст: электронный

Рецидив принято разделять на общий и специальный. Общий рецидив предусматривает совершение лицом разнородных преступлений. Специальный рецидив предусматривает совершение лицом однородных или одинаковых преступлений. Все преступные деяния, являющиеся по итогу «множественными», должны быть совершены одним и тем же лицом, причем независимо от того, какую роль лицо исполняло в этих деяниях.

Ключевое значение множественности заключается в том, что она, усиливает или уже ужесточает уголовную ответственность за последующее деяние. Основанием для усиления выступает повышенная степень общественной опасности лица, совершившего, таким образом, несколько преступлений. Совершение лицом нескольких преступлений подряд позволяет ему получить так необходимый ему преступный опыт, который в дальнейшем облегчает ему преступную деятельность, тем самым повышая исходящую от него опасность для людей, общества и государства опасность, а также позволяет ему найти способы укрыться от ответственности, что в конечном счете порождает сформировавшуюся стойкую антиобщественную и общественно вредную личность.

Реальную совокупность преступлений образует совершение лицом нескольких деяний двух или более различных видов преступлений. В таком случае, как известно, каждое из совершенных преступлений квалифицируется по самостоятельной статье Особенной части УК РФ.

При квалификации деяний по совокупности преступлений, ответственность за которые предусмотрена ст. 158 УК РФ, с преступлениями против безопасности компьютерной информации необходимо обратить внимание на наличие разъяснений, данных Пленумом Верховного Суда РФ от 27.12.2002 г. № 29 «О судебной практике по делам о краже, грабеже и разбое»[1]

// Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562612 (дата обращения 29.04.2025)

[1] О судебной практике по делам о краже, грабеже и разбое: Постановление Пленума Верховного Суда РФ от 27.12.2002 N 29 (ред. от 15.12.2022) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_40412/

При квалификации деяния по признакам составов преступлений, ответственность за которые предусмотрена статьи. 159^6 и 272 УК РФ, следует иметь в виду, что ответственность по данным статьям предусмотрена за совершение различных противоправных действий, с учетом различной объективной стороны преступлений. При совершении лицом деяния, имеющего все признаки компьютерного мошенничества путем удаления, блокирования, модификации либо копирования компьютерной информации, необходимо установить наличие неправомерного доступа к охраняемой законом компьютерной информации. Если такие признаки установлены, то необходима квалификация действия лица как идеальной совокупности преступлений. Следует отметить - из положения ст. 159^6 УК РФ, основным объектом уголовно-правовой охраны является собственность, а дополнительным – компьютерная безопасность.

При осуществлении компьютерного мошенничества санкции необходимо сопоставлять с частью второй ст. 272 УК РФ, а не частью первой, как совершаемое с корыстной заинтересованностью, за которое максимальная санкция установлена в размере до 4 лет лишения свободы[1].

Таким образом, нельзя ставить знак равенства между компьютерным мошенничеством, совершенным путем удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование компьютерной техники (в т.ч. копирования компьютерной информации), и неправомерным доступом к компьютерной информации (ст. 272 УК РФ). Поэтому квалификация деяния только по ч. 1 ст. 159^6 УК РФ не отражает в полной мере общественную опасность совершаемого деяния и требует, как

[1] Подройкина И. А. Уголовное право. Особенная часть. Семестр I: учебник для вузов / ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 556 с. — (Высшее образование). — ISBN 978-5-534-16720-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561883 (дата обращения 02.05.2025)

уже говорилось, квалификации по совокупности преступлений при наличии соответствующих оснований.

Квалификацию по реальной совокупности преступлений, ответственность за которые предусмотрена статьями 272 и 165 УК РФ, могут образовывать случаи использования лицами чужих аутентификационных данных, полученных путем обмана или злоупотребления доверием, для дальнейшего безвозмездного доступа в сеть Интернет или безвозмездного пользования любыми другими услугами в сети Интернет.

При конкуренции основного и квалифицированного составов преступления против безопасности компьютерной информации квалификация производится по части статьи УК РФ, предусматривающей ответственность за квалифицированное деяние. В случае конкуренции между собой специальных норм квалификация должна производиться по норме, предусматривающей более тяжкий квалифицирующий признак.

ЗАКЛЮЧЕНИЕ

В процессе проведенного исследования были получены следующие выводы:

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

2. Преступления в сфере компьютерной информации – это запрещенные уголовным законом Российской Федерации виновно совершенные

общественно опасные деяния, причиняющие вред или создающие опасность причинения вреда безопасности обращения компьютерной информации или вреда критической информационной инфраструктуре Российской Федерации.

3. Компьютерная преступность представляет собой противоправное и негативное социальное явление, совокупность всех преступлений, в рамках которой используются либо атакуются компьютер, компьютерная сеть или отдельно взятое сетевое устройство. Устойчивая тенденция возрастания общественной опасности компьютерных преступлений обусловлена стремительным расширением сфер использования информационных технологий и, в частности компьютерной техники экономической, политической, военной областях и др. Соответственно, российской уголовное законодательство в данной сфере не в полной мере отвечает потребностям практики и требует дальнейшего совершенствования составов компьютерных преступлений.

С каждым годом фиксируется рост преступлений, совершаемы в сфере высоких технологий. Так, по данным МВД России в 2024 году 40% преступлений были совершены с использованием информационно-телекоммуникационных технологий. Таких деяний зарегистрировано на 13,1 % больше, чем в 2023 году, в том числе тяжких и особо тяжких составов – на 7,8 %. Исходя из данной статистики, можно сделать вывод о том, что уголовно-правовое законодательство отстает в вопросе совершения киберпреступлений.

4. В дипломной работе обоснована целесообразность изменения наименования главы 28 УК РФ на: «Преступления против безопасности компьютерной информации».

5. Основным объектом преступлений в сфере компьютерной информации являются конкретные общественные отношения, возникающие в той или иной плоскости оборота компьютерной информации. Объективная сторона выражается активными действиями. Субъектом выступает 16-летнее, вменяемое физическое лицо, однако в некоторых случаях выступает

специальный субъект – должностное лицо. Субъективная сторона выражена умыслом.

6. Предложено авторское определение термина «киберпреступность». В рамках данной дипломной работы под киберпреступностью мы понимаем совокупность всех преступлений, в рамках которой используются либо атакуются компьютер, компьютерная сеть или отдельно взятое сетевое устройство.

7. Обоснована необходимость привлечения к уголовной ответственности пользователей искусственного интеллекта, используемого с целью совершения преступлений.

8. Предлагается авторская редакция ч. 1 ст. 272 УК РФ «Неправомерный доступ к компьютерной информации» в следующей редакции:

Доступ к охраняемой компьютерной информации, если это деяние повлекло неправомерно удаление, блокирование, модификацию либо копирование компьютерной информации, - …» далее по тексту;

9. Предлагается использовать для целей применения уголовного закона только понятие «Компьютерное устройство», без использования понятия «ЭВМ».

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

I. Законы, нормативно-правовые акты и иные официальные документы

1. Уголовный кодекс Российской Федерации от 13.06.1996 N 63-ФЗ (ред. от 21.04.2025) (с изм. и доп., вступ. в силу с 02.05.2025) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 01.03.2025).

2. Кодекс Российской Федерации об административных правонарушениях от 30.12.2001 N 195-ФЗ (ред. от 07.04.2025) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_34661/01db86fb46c88f00ff06171e17bb7d66fcf09a53/ (дата обращения 10.05.2025). (дата обращения 07.03.2025).

3. Гражданский кодекс Российской Федерации (часть четвертая) от 18.12.2006 N 230-ФЗ (ред. от 22.07.2024) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_64629/ce1359ed5b9bd99896d7a496c7887e7c223a2cbc/ (дата обращения 10.05.2025).

4. О связи: Федеральный закон от 07.07.2003 N 126-ФЗ // СПС «Консультант плюс». - https://www.consultant.ru/document/cons_doc_LAW_43224/b819c620a8c698de35861ad4c9d9696ee0c3ee7a/ (дата обращения 10.05.2025).

5. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27.07.2006 N 149-ФЗ // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_61798/c5051782233acca771e9adb35b47d3fb82c9ff1c/ (дата обращения 10.05.2025). (дата обращения 01.03.2025).

6. О персональных данных: Федеральный закон от 27.07.2006 N 152-ФЗ // СПС «Консультант плюс». - https://www.consultant.ru/document/cons_doc_LAW_61801/4f41fe599ce341751e4e34dc50a4b676674c1416/. (дата обращения 12.05.2025).

7. О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона О безопасности критической информационной инфраструктуры Российской Федерации»: Федеральный закон от 26.07.2017 г. № 194-ФЗ // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_220891/ (дата обращения 13.05.2025).

8. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон от 26.07.2017 N 187-ФЗ // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 12.05.2025).

9. О внесении изменений в Уголовный кодекс Российской Федерации и отдельные законодательные акты Российской Федерации о: Федеральный закон т 07.12.2011 N 420-ФЗ // СПС «Консультант плюс». - URL:

https://www.consultant.ru/document/cons_doc_LAW_122864/ (дата обращения 09.04.2025).

10. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации: Федеральный закон от 14.07.2022 N 260-ФЗ (последняя редакция) // СПС «Консультант плюс». URL: https://www.consultant.ru/document/cons_doc_LAW_421797/3d0cac60971a511280cbba229d9b6329c07731f7/Федеральный закон (дата обращения 09.04.2025).

11. О внесении изменений в Уголовный кодекс Российской Федерации: Федеральный закон от 30.11.2024 N 421-ФЗ https://www.consultant.ru/document/cons_doc_LAW_491931/(дата обращения 09.04.2025).

12. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 N 400 // СПС «Консультант плюс». – URL: https://www.consultant.ru/document/cons_doc_LAW_389271/ (дата обращения 10.05.2025).

13. Computer Misuse Act 1990: call for information – Акт о компьютерных злоупотреблениях Великобритании. Официальный сайт Правительства Великобритании // https://www.gov.uk/government/consultations/computer-misuse-act-1990-call-for-information. (дата обращения 06.03.2025).

14. Уголовный кодекс Федеративной республики Германии. Перевод Головненков П. В. URL: // https://www.unipotsdam.de/fileadmin/projects/lshellmann/Forschungsstelle_Russisches_Recht/Neuauflage_der_kommentierten_StGB%C3%9Cbersetzung_von_Pavel_Golovnenkov.pdf. (дата обращения 06.03.2025).

15. Уголовный кодекс Ирландии Официальный сайт Правительства Великобритании // URL: https://www.legislation.gov.uk/apni/1966/20/section/8

16. Уголовный кодекс Нидерландов Официальный сайт Правительства Нидерландов // URL: https://www.government.nl/ (дата обращения 06.03.2025).

II. Монографии, учебники, учебные пособия

17. Бавсун, *М. В.* Квалификация преступлений по признакам субъективной стороны: учебник для вузов / М. В. Бавсун, С. В. Векленко. — 2-е изд., испр. и доп. — Москва: Издательство Юрайт, 2025. — 143 с. — (Высшее образование). — ISBN 978-5-534-18049-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/index.php/bcode/563066 (дата обращения 10.04.2025).

18. Бастрыкин А. И. Уголовное право. Особенная часть: учебник для вузов / под общей редакцией А. И. Бастрыкина; под научной редакцией А. И. Чучаева. — Москва: Издательство Юрайт, 2025. — 468 с. — (Высшее образование). — ISBN 978-5-534-12079-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/580312. (дата обращения 21.04.2025).

19. Батурин Ю. М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. 159 с. URL: https://spblib.ru/ru/catalog/-/books/11477840-komp-yuternaya-prestupnost-i-komp-yuternaya-bezopasnost- (дата обращения 16.03.2025).

20. Батурин Ю. М. Проблемы компьютерного права. - М.: Юриздат, 1991. 109 с. URL: https://lib.dm-centre.ru/lib/document/gpntb/ESVODT/44c8fb92a7d519334f5e32dcb77174cf/ (дата обращения 21.05.2025).

21. Бекряшев А. К., Белозеров И. П. Теневая экономика и экономическая преступность, 2003. 149 с. Текст: электронный //URL: https://knigogid.ru/books/1907184-tenevaya-ekonomika-i-ekonomicheskaya-prestupnost/toread (дата обращения 28.03.2025).

22. Беришвили Р.Ш., Чакрян В.Р. Компьютерные преступления // Международный научный журнал «Символ науки» № 12-1 / 2021. С. 53.

23. Большой толковый словарь русского языка URL: - https://gramota.ru/poisk?query=информация&mode=slovari&dicts [] =42 (дата обращения 01.03.2025).

24. Боровиков, В. Б. Уголовное право. Общая часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов; под редакцией В. Б. Боровикова. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 243 с. — (Высшее образование). — ISBN 978-5-534-19802-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561008. (дата обращения 24.03.2025).

25. Боровиков, В. Б. Уголовное право. Особенная часть: учебник для вузов / В. Б. Боровиков, А. А. Смердов; под редакцией В. Б. Боровикова. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 505 с. — (Высшее образование). — ISBN 978-5-534-17301-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/536930 (дата обращения 24.03.2025).

26. Векленко В. В. Уголовное право. Общая часть: учебник для вузов / под общей редакцией Векленко В. В. — 3-е изд. — Москва: Издательство Юрайт, 2025. — 512 с. — (Высшее образование). — ISBN 978-5-534-15530-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562995 (дата обращения 27.03.2025).

27. Гладких, В. И. Уголовное право России в таблицах и комментариях. Общая часть: учебник для среднего профессионального образования / В. И. Гладких, М. Г. Решняк. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 212 с. — (Профессиональное образование). — ISBN 978-5-534-17477-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/568689 (дата обращения 15.04.2025).

28. Гладких В. И. Уголовное право. Особенная часть: преступления против общественной безопасности и общественного порядка: учебник для вузов / под общей редакцией Гладких В. И., Есаяна А. К. — Москва: Издательство Юрайт, 2025. — 352 с. — (Высшее образование). — ISBN 978-5-534-13708-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/567546 (дата обращения 15.04.2025).

29. Голованова, Н. А. Уголовное право Англии: учебник для вузов / Н. А. Голованова. — Москва: Издательство Юрайт, 2025. — 188 с. — (Высшее образование). — ISBN 978-5-9916-8869-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561351 (дата обращения 06.03.2025).

30. Гриб Г.В., Тюнис И.О. Криминалистика и цифровые технологии: научный журнал / Российский следователь, 2020. – №9. – С. 156 – 160.

31. Диканова Т. А., Ображиев К. В. Уголовное право России. Особенная часть. Том 2. М.: Юрайт. 2023. 640 с. Текст: электронный // URL: https://search.rsl.ru/ru/record/01010335420 (дата обращения 18.04.2025)

32. Есаков Г. А. Российское уголовное право. Особенная часть. М.: Проспект. 2023. 656 с. Текст: электронный // URL: https://www.labirint.ru/books/989332/?ysclid=mbxq7ljy9c936175081 (дата обращения 25.04.2025)

33. Капинус О. С. Уголовное право России. Особенная часть: учебник для вузов — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2024. — 1189 с. — (Высшее образование). — ISBN 978-5-534-18351-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/534839 (дата обращения 23.04.2025)

34. Козаченко, И. Я. Уголовное право. Общая часть: учебник для вузов / И. Я. Козаченко, Г. П. Новоселов. — 7-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 400 с. — (Высшее образование). — ISBN 978-5-534-20751-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/558681 (дата обращения 08.04.2025)

35. Козаченко И. Я. Уголовное право. Особенная часть. Краткий курс: учебник для вузов / ответственный редактор И. Я. Козаченко. — Москва: Издательство Юрайт, 2025. — 263 с. — (Высшее образование). — ISBN 978-5-534-18051-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/560123 (дата обращения 09.04.2025)

36. Крылова Н. Е. Уголовное право зарубежных стран. Общая часть: учебник для вузов / ответственный редактор Н. Е. Крылова. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 576 с. — (Высшее образование). — ISBN 978-5-534-18747-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/578970 (дата обращения 07.03.2025)

37. Крылова Н. Е. Уголовное право зарубежных стран. Особенная часть: учебник для вузов / ответственный редактор Н. Е. Крылова. — 5-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 397 с. — (Высшее образование). — ISBN 978-5-534-16218-9. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561346 (дата обращения 07.03.2025)

38. Леонтьев Б. К. Хакеры, взломщики и другие информационные убийцы. – М.: Майор (Осипенко), 2001 – 190 с. Текст: электронный URL: https://lib.ru/TECHBOOKS/LEONTIEV/hakery.txt (дата обращения 22.03.2025)

39. Медведев, Е. В. Уголовное право России. Общая часть: учебное пособие для вузов / Е. В. Медведев. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 221 с. — (Высшее образование). — ISBN 978-5-534-18080-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/534237. (дата обращения 09.04.2025)

40. Минаев С. В. Компьютерные преступления: сущность, особенности и возможности предотвращения // NOMOTHETIKA: Философия. Социология. Право. 2017. №24 (273). URL: https://cyberleninka.ru/article/n/kompyuternye-prestupleniya-suschnost-osobennosti-i-vozmozhnosti-predotvrascheniya (дата обращения: 09.05.2025).

41. Наумов А. В., Кибальник А. Г. Преступления против общественной безопасности и общественного порядка: учебник для вузов / ответственные редакторы А. В. Наумов, А. Г. Кибальник. — 6-е изд., перераб. и доп. — Москва: Юрайт, 2025. — 158 с. — (Высшее образование). — ISBN 978-5-534-18589-8. — Текст: электронный // Образовательная платформа Юрайт [сайт]. с. 158 — URL: https://urait.ru/bcode/563347/p.158 (дата обращения: 01.05.2025).

42. Наумов А. В., Кибальник А. Г. Уголовное право. Общая часть: учебник для вузов / ответственные редакторы. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 448 с. — (Высшее образование). — ISBN 978-5-534-18585-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/562612 (дата обращения 29.04.2025)

43. Ожегов С.И., Н.Ю. Шведова. Толковый словарь русского языка. – М.: Академия наук СССР, 1949. С. 398.

44. Подройкина И. А. Уголовное право. Особенная часть. Семестр I: учебник для вузов / ответственные редакторы И. А. Подройкина, Е. В. Серегина, С. И. Улезько. — 6-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 556 с. — (Высшее образование). — ISBN 978-5-534-16720-7. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561883 (дата обращения 02.05.2025).

45. Рарог А.И. Общая часть учебник издание второе переработанное и дополненное. Под редакцией доктора юридических наук, профессора Рарога А.И, профессора Чучаева А.И. // Образовательная платформа ALL Адвокатура [сайт]. с. 558 URL: https://all-advokatura.ru/upload/iblock/c21/c2111d8ca95fddb9f46da5ea203966b7.pdf (дата обращения 02.05.2025).

46. Савельев Д. В. Соучастие в преступлении. Преступная группа: учебник для вузов / Д. В. Савельев. — 3-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 134 с. — (Высшее образование). — ISBN 978-

5-534-17840-1. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/565269. (дата обращения 27.04.2025)

47. Савельев Д. В. Уголовное право. Общая часть: учебник для вузов / Д. В. Савельев. — Москва: Издательство Юрайт, 2025. — 374 с. — (Высшее образование). — ISBN 978-5-534-21540-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/575502 (дата обращения 06.05.2025).

48. Сверчков В. В. Уголовное право. Общая часть. Учебно-методический комплекс: учебник для вузов / В. В. Сверчков. — Москва: Издательство Юрайт, 2025. — 649 с. — (Высшее образование). — ISBN 978-5-534-11726-4. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/566527. (дата обращения 08.05.2025).

49. Сверчков В. В. Уголовное право. Особенная часть: учебник для среднего профессионального образования / В. В. Сверчков. — 12-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2025. — 421 с. — (Профессиональное образование). — ISBN 978-5-534-20225-0. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/557823 (дата обращения12.05.2025).

50. Седаков С.Ю., Филиппова Т. П. Хрестоматия по всеобщей истории государства и права. - М.: Юрист, 1996. - 391 с. Текст: электронный // Юридическая научная библиотека издательства СПАРК [сайт]. — URL: http://jurinica.ru/catalog/pravo/teoriya-i-istoriya-prava-i-gosudarstva-istoriya-pravovyx-uchenij/xrestomatiya-po-vseobshhej-istorii-gosudarstva_goods_18100/ (дата обращения 14.03.2025).

51. Серебренникова А. В. Уголовное право Германии: учебник для вузов / А. В. Серебренникова. — Москва: Издательство Юрайт, 2025. — 124 с. — (Высшее образование). — ISBN 978-5-534-10123-2. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/561354 (дата обращения09.03.2025)

III. Диссертации, авторефераты диссертаций

52. Гайфутдинов Р.Р. Понятие и квалификация преступлений против безопасности компьютерной информации // Автореф. дисс. на соиск. ученой степени канд.юрид.наук. – Казань: Изд-во Казанского (Приволжского) федерального университета, 2017. 26 с.

53. Евдокимов К.Н. Противодействие компьютерной преступности: теория, законодательство, практика // Дисс. на соис. ученой степени докт.юрид наук. М.: Изд-во института Прокуратуры РФ, 2011. 557.

54. Капырюлин А.А. Преступления в сфере компьютерной информации: уголовно-правовой и криминологический апекты // Дисс. на соис. ученой степени докт.юрид наук. – Тамбов, 2007. 29 с.

IV. Материалы практики

55. О судебной практике по делам о краже, грабеже и разбое: Постановление Пленума Верховного Суда РФ от 27.12.2002 N 29 (ред. от 15.12.2022) // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_40412/ (дата обращения 13.04.2025).

56. О некоторых вопросах судебной практики по уголовным делам о преступлениях в сфере компьютерной информации, а также иных преступлениях, совершенных с использованием электронных или информационно-телекоммуникационных сетей, включая сеть "Интернет" Постановление Пленума Верховного Суда РФ от 15.12.2022 N 37 // СПС «Консультант плюс». - URL: https://www.consultant.ru/document/cons_doc_LAW_434573/ (дата обращения 17.05.2025).

57. Краткая характеристика состояния преступности в Российской Федерации за январь - декабрь 2024 года // МВД РФ. Официальный сайт – URL: https://мвд.рф/reports/item/60248328/ (дата обращения 01.03.2025).

58. Приговор Фрунзенского районного суда г. Владимира №1-199/2024 от 23.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/rUi0IOY5QI5J/ (дата обращения 24.024.2025).

59. Приговор Первомайского районного суда г. Новосибирска №1-436/2024 от 24.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/8HG5DkwEmsVJ/ (дата обращения 27.04.2025).

60. Приговор Октябрьского районного суда г. Иваново № 1-308/2024 от 28.12.2024 // Интернет-ресурс СудАкт – URL: https://sudact/ru/regular/doc/sr7cmrYRke1V/ (дата обращения 22.04.2025).