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

Департамент публичного права
(наименование)

40.03.01 Юриспруденция
(код и наименование направлению подготовки / специальности)

Уголовно-правовой
(направленность (профиль) / специализация)

# ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (БАКАЛАВРСКАЯ РАБОТА)

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

Обучающийся М.А. Гаврильченко
(Инициалы Фамилия) (личная подпись)

Руководитель канд. юрид. наук, доцент, Т.Ю. Дементьева
(ученая степень (при наличии), ученое звание (при наличии), Инициалы Фамилия)

Тольятти 2025

## Аннотация

Актуальность темы исследования обусловлена стремительным развитием информационных технологий, которые в современном мире играют ключевую роль практически во всех сферах жизнедеятельности общества. Цифровизация экономики, государственного управления, социальной сферы и повседневной жизни граждан создает не только новые возможности, но и порождает специфические угрозы, связанные с использованием информационно-телекоммуникационных технологий в противоправных целях. Компьютерная преступность стала одним из наиболее динамично развивающихся видов преступности, представляющим серьезную угрозу национальной безопасности, экономическим интересам государства, правам и законным интересам граждан.

В этих условиях особую значимость приобретает эффективное правовое регулирование отношений в сфере информационной безопасности, в том числе посредством установления уголовной ответственности за наиболее опасные посягательства на компьютерную информацию. Российское уголовное законодательство в данной сфере прошло значительный путь развития: от отсутствия специальных норм до формирования самостоятельной главы в Особенной части Уголовного кодекса РФ, посвященной преступлениям в сфере компьютерной информации. Однако стремительное развитие информационных технологий и появление новых форм общественно опасных деяний требуют постоянного совершенствования уголовно-правовых норм и практики их применения.

Объектом исследования являются общественные отношения, возникающие в связи с установлением и реализацией уголовной ответственности за преступления в сфере компьютерной информации.

Предметом исследования выступают нормы уголовного законодательства, предусматривающие ответственность за преступления в сфере компьютерной информации, материалы судебной практики, а также

научные концепции и теоретические положения, касающиеся данной проблематики.

Цель исследования состоит в комплексном анализе теоретических и практических проблем уголовной ответственности за преступления в сфере компьютерной информации и разработке на этой основе предложений по совершенствованию уголовного законодательства и практики его применения.

Для достижения указанной цели были поставлены следующие задачи:

- исследовать основные этапы исторического развития законодательства о преступлениях в сфере компьютерной информации;
- раскрыть понятие и сущность компьютерной преступности в современном обществе;
- сформулировать понятие преступлений в сфере компьютерной информации и выявить их особенности;
- проанализировать объективные признаки составов компьютерных преступлений;
- исследовать субъективные признаки составов компьютерных преступлений;
- разработать систему мер противодействия компьютерной преступности.

Структура работы обусловлена целью и задачами исследования и включает в себя введение, три главы, объединяющие семь параграфов, заключение и список использованной литературы и используемых источников.

## Оглавление

Введение ..... 4
Глава 1 Характеристика преступлений в сфере компьютерной информации.. 8
1.1 Основные этапы исторического развития законодательства о преступлениях в сфере компьютерной информации ..... 8
1.2 Понятие и сущность компьютерной преступности в обществе..... 13
1.3 Понятие преступлений в сфере компьютерной информации, их особенности ..... 20
Глава 2 Уголовно-правовая характеристика компьютерных преступлений .. 29
2.1 Объективные признаки компьютерных преступлений ..... 29
2.2 Субъективные признаки компьютерных преступлений..... 37
2.3 Квалифицирующие признаки преступлений в сфере компьютерной информации ..... 49
Глава 3 Организация и система мер противодействия компьютерной преступности ..... 56
Заключение ..... 69
Список используемой литературы и используемых источников ..... 78

# Введение

Актуальность темы исследования обусловлена стремительным развитием информационных технологий, которые в современном мире играют ключевую роль практически во всех сферах жизнедеятельности общества. Цифровизация экономики, государственного управления, социальной сферы и повседневной жизни граждан создает не только новые возможности, но и порождает специфические угрозы, связанные с использованием информационно-телекоммуникационных технологий в противоправных целях. Компьютерная преступность стала одним из наиболее динамично развивающихся видов преступности, представляющим серьезную угрозу национальной безопасности, экономическим интересам государства, правам и законным интересам граждан.

Современные компьютерные преступления характеризуются высоким уровнем латентности, транснациональным характером, значительным материальным ущербом и сложностью выявления, расследования и предупреждения. По данным экспертов, ежегодные потери мировой экономики от киберпреступности исчисляются триллионами долларов, а их рост значительно опережает темпы роста глобальной экономики. Российская Федерация также сталкивается с серьезными вызовами в сфере информационной безопасности, о чем свидетельствует постоянный рост числа зарегистрированных преступлений в сфере компьютерной информации и преступлений, совершаемых с использованием информационно-телекоммуникационных технологий.

В этих условиях особую значимость приобретает эффективное правовое регулирование отношений в сфере информационной безопасности, в том числе посредством установления уголовной ответственности за наиболее опасные посягательства на компьютерную информацию. Российское уголовное законодательство в данной сфере прошло значительный путь развития: от отсутствия специальных норм до формирования самостоятельной

главы в Особенной части Уголовного кодекса РФ, посвященной преступлениям в сфере компьютерной информации. Однако стремительное развитие информационных технологий и появление новых форм общественно опасных деяний требуют постоянного совершенствования уголовно-правовых норм и практики их применения.

Степень научной разработанности темы исследования характеризуется наличием значительного количества научных трудов, посвященных различным аспектам уголовной ответственности за преступления в сфере компьютерной информации. Теоретические основы правового регулирования, характеристики отдельных составов компьютерных преступлений анализировались в работах С.Д. Бражника, Н.Г. Шурухнова, А.Л. Осипенко, В.И. Гладких и др.

При этом, несмотря на значительное количество научных исследований, в данной области остается ряд дискуссионных вопросов, требующих теоретического осмысления. К ним относятся проблемы определения понятия и сущности компьютерной преступности, уголовно-правовой оценки новых форм общественно опасных деяний, совершаемых с использованием информационных технологий, отграничения преступлений в сфере компьютерной информации от смежных составов преступлений, а также вопросы совершенствования системы мер противодействия компьютерной преступности.

Объектом исследования являются общественные отношения, возникающие в связи с установлением и реализацией уголовной ответственности за преступления в сфере компьютерной информации.

Предметом исследования выступают нормы уголовного законодательства, предусматривающие ответственность за преступления в сфере компьютерной информации, материалы судебной практики, а также научные концепции и теоретические положения, касающиеся данной проблематики.

Цель исследования состоит в комплексном анализе теоретических и практических проблем уголовной ответственности за преступления в сфере компьютерной информации и разработке на этой основе предложений по совершенствованию уголовного законодательства и практики его применения.

Для достижения указанной цели были поставлены следующие задачи:

- исследовать основные этапы исторического развития законодательства о преступлениях в сфере компьютерной информации;
- раскрыть понятие и сущность компьютерной преступности в современном обществе;
- сформулировать понятие преступлений в сфере компьютерной информации и выявить их особенности;
- проанализировать объективные признаки составов компьютерных преступлений;
- исследовать субъективные признаки составов компьютерных преступлений;
- разработать систему мер противодействия компьютерной преступности.

Методологическую основу исследования составляет совокупность общенаучных и частнонаучных методов познания, включая диалектический, исторический, системный, формально-логический, сравнительно-правовой, статистический и другие методы.

Нормативной базой исследования послужили Конституция Российской Федерации, международные правовые акты, Уголовный кодекс Российской Федерации, иные федеральные законы и подзаконные нормативные правовые акты, регулирующие отношения в сфере информационной безопасности.

Структура работы обусловлена целью и задачами исследования и включает в себя введение, три главы, объединяющие семь параграфов, заключение и список использованной литературы и используемых источников.

# Глава 1 Характеристика преступлений в сфере компьютерной информации

## 1.1 Основные этапы исторического развития законодательства о преступлениях в сфере компьютерной информации

Историческое развитие законодательства о преступлениях в сфере компьютерной информации тесно связано с эволюцией информационных технологий и их внедрением в различные сферы общественной жизни. Осмысление процесса формирования правовых норм, направленных на противодействие компьютерной преступности, имеет важное значение для понимания современного состояния уголовного законодательства и определения перспектив его дальнейшего совершенствования. Генезис правового регулирования в данной области характеризуется поэтапным развитием, обусловленным как технологическими изменениями, так и трансформацией представлений о характере и степени общественной опасности деяний, совершаемых с использованием компьютерных технологий [3, с. 53].

Первый этап формирования законодательства о преступлениях в сфере компьютерной информации охватывает период с конца 1960-х до начала 1980-х годов и связан с появлением первых случаев противоправного использования компьютерных технологий. В эти годы компьютерные системы еще не получили широкого распространения и использовались преимущественно в научных, военных и финансовых учреждениях. Случаи неправомерного доступа к компьютерной информации были относительно редкими и квалифицировались в рамках уже существующих составов преступлений, таких как кража, мошенничество, промышленный шпионаж или нарушение неприкосновенности частной жизни. Первые специальные нормы, направленные на противодействие компьютерным преступлениям, появились в законодательстве Швеции (1973 г.) и США (штат Флорида,

1978 г.). В США на федеральном уровне был принят Закон о защите федеральных компьютерных систем (1977 г.), однако он имел весьма ограниченную сферу применения и не предусматривал уголовной ответственности за все виды компьютерных преступлений [12, с. 76].

Второй этап развития законодательства о преступлениях в сфере компьютерной информации приходится на 1980-е – начало 1990-х годов и характеризуется активным формированием специальных правовых норм, криминализирующих различные формы неправомерного использования компьютерных технологий. В этот период происходит широкое распространение персональных компьютеров, развитие локальных сетей и начало массового использования интернета, что создает новые возможности для совершения противоправных деяний [10, с. 92]. В США был принят Закон о компьютерном мошенничестве и злоупотреблениях (1984 г.), в Великобритании – Закон о злоупотреблении компьютером (1990 г.), в Германии – Второй закон по борьбе с экономической преступностью (1986 г.), включивший в Уголовный кодекс ФРГ несколько новых составов преступлений, связанных с компьютерной информацией. В это же время появляются первые международные документы, посвященные проблемам компьютерной преступности, в частности, Рекомендация № R(89)9 Комитета министров Совета Европы «О преступлениях, связанных с компьютерами» (1989 г.), которая предлагала государствам-членам включить в национальное законодательство уголовную ответственность за определенные виды компьютерных преступлений.

В Советском Союзе и на постсоветском пространстве второй этап развития законодательства о преступлениях в сфере компьютерной информации имел свои особенности. В уголовном законодательстве СССР не содержалось специальных норм, предусматривающих ответственность за компьютерные преступления, хотя определенные формы противоправного использования ЭВМ могли быть квалифицированы по общим статьям УК РСФСР, таким как хищение государственного или общественного имущества,

злоупотребление служебным положением, нарушение правил охраны труда. Первые специальные нормы, устанавливающие уголовную ответственность за преступления в сфере компьютерной информации, появились в проекте Основ уголовного законодательства Союза ССР и республик 1991 года, которые так и не вступили в силу из-за распада Советского Союза. В дальнейшем эти положения были учтены при разработке уголовных кодексов новых независимых государств [19, с. 60].

Третий этап формирования законодательства о преступлениях в сфере компьютерной информации охватывает середину 1990-х – начало 2000-х годов и характеризуется систематизацией и унификацией правовых норм в данной области, а также расширением международного сотрудничества в борьбе с киберпреступностью [18, с. 129]. В этот период компьютерные технологии и интернет становятся неотъемлемой частью повседневной жизни, что приводит к значительному росту числа компьютерных преступлений и появлению их новых форм. В Российской Федерации данный этап ознаменовался принятием Уголовного кодекса 1996 года, в котором впервые была выделена самостоятельная глава 28 «Преступления в сфере компьютерной информации», включающая три статьи: ст. 272 «Неправомерный доступ к компьютерной информации», ст. 273 «Создание, использование и распространение вредоносных программ для ЭВМ» и ст. 274 «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Аналогичные нормы были включены в уголовные кодексы других государств постсоветского пространства.

Важным событием третьего этапа стало принятие в 2001 году Конвенции Совета Европы о преступности в сфере компьютерной информации (Будапештской конвенции), которая установила минимальные стандарты национального законодательства в области криминализации компьютерных преступлений, определила принципы международного сотрудничества в борьбе с киберпреступностью и предложила механизмы взаимной правовой помощи при расследовании компьютерных преступлений. Несмотря на то, что

Российская Федерация не ратифицировала данную конвенцию, многие ее положения учитывались при дальнейшем совершенствовании отечественного уголовного законодательства [9, с. 65].

Четвертый этап развития законодательства о преступлениях в сфере компьютерной информации начался в середине 2000-х годов и продолжается по настоящее время. Он характеризуется адаптацией правовых норм к новым вызовам цифровой эпохи, таким как массовое распространение социальных сетей, облачных технологий, мобильных устройств, интернета вещей, а также усилением транснационального характера компьютерной преступности. В этот период в уголовном законодательстве многих государств появляются новые составы преступлений, связанные с использованием информационно-телекоммуникационных сетей, в том числе для распространения противоправного контента, организации несанкционированного доступа к защищенным системам, хищения персональных данных и иных видов киберпреступлений.

На заключительной стадии эволюции российского законодательства произошла фундаментальная трансформация нормативно-правовой базы в области компьютерно-информационных преступлений. Существенные модификации были внедрены Федеральным законом № 420-ФЗ от 07.12.2011, который значительно реструктурировал главу 28 УК РФ, переработав как содержательные элементы, так и карательные меры статей 272-274, с детальным уточнением квалифицирующих характеристик преступных деяний. Законодательный массив пополнился статьей 274.1 в 2012 году, регламентирующей правовые последствия противоправных действий в отношении критической информационной инфраструктуры РФ, а также статьей 274.2 (2017 год), устанавливающей уголовно-правовые санкции за нарушения в сфере централизованного управления коммуникационными сетями России. Параллельно произошла криминализация ряда деяний, сопряженных с эксплуатацией информационно-телекоммуникационных сетей при совершении различных преступлений, включая мошеннические действия

с применением электронных платежных инструментов, публичное подстрекательство к террористической активности, умышленное распространение заведомо недостоверных сведений.

В глобальном контексте четвертая фаза ознаменовалась формированием комплексной международно-правовой архитектуры противодействия компьютерной преступности. Ключевыми элементами данной системы стали: Конвенция Совета Европы о защите несовершеннолетних от сексуальной эксплуатации и сексуальных злоупотреблений (2007), межгосударственное Соглашение стран СНГ по борьбе с компьютерными преступлениями (2001), многостороннее Соглашение государств-членов ШОС об обеспечении международной информационной безопасности (2009). Под эгидой Организации Объединенных Наций был сформирован специализированный экспертный орган по исследованию проблематики киберпреступности, осуществляющий разработку методологических рекомендаций по унификации национальных правовых систем и интенсификации межгосударственной кооперации в рассматриваемой области [7, с. 188].

Анализируя основные этапы исторического развития законодательства о преступлениях в сфере компьютерной информации, следует отметить его динамичный характер и постоянную адаптацию к новым технологическим вызовам. При этом правовое регулирование в данной области развивается в двух основных направлениях: с одной стороны, происходит криминализация новых форм противоправного поведения, связанных с использованием информационных технологий, с другой – совершенствуются механизмы международного сотрудничества в борьбе с компьютерной преступностью. Вместе с тем, несмотря на значительный прогресс в развитии законодательства о преступлениях в сфере компьютерной информации, оно по-прежнему сталкивается с рядом вызовов, обусловленных транснациональным характером киберпреступности, анонимностью интернета, сложностью обнаружения и фиксации цифровых следов, а также

различиями в национальных подходах к криминализации отдельных видов деяний [5, с. 43].

Современное состояние законодательства о преступлениях в сфере компьютерной информации характеризуется тенденцией к расширению круга охраняемых общественных отношений и усилению уголовно-правовой защиты информационной безопасности. При этом наблюдается определенное смещение акцентов с защиты собственно компьютерной информации на обеспечение безопасности критической информационной инфраструктуры, защиту персональных данных и противодействие использованию информационных технологий в террористических и экстремистских целях. Данная тенденция отражает осознание возрастающей роли информационной безопасности в обеспечении национальной безопасности государства и защите прав и свобод граждан.

Таким образом, исторический путь развития законодательства о преступлениях в сфере компьютерной информации представляет собой сложный и многогранный процесс, обусловленный как эволюцией информационных технологий, так и изменением представлений о характере и степени общественной опасности различных форм противоправного поведения в информационной сфере. Изучение этого процесса позволяет лучше понять логику формирования современного уголовного законодательства и определить перспективные направления его дальнейшего совершенствования с учетом новых вызовов и угроз информационной безопасности.

## 1.2 Понятие и сущность компьютерной преступности в обществе

Компьютерная преступность представляет собой сложное социально-правовое явление, возникшее и эволюционирующее вместе с развитием информационных технологий и их проникновением во все сферы общественной жизни. В современных условиях глобальной цифровизации

данный вид преступности приобретает особую актуальность, ставя перед наукой уголовного права и правоприменительной практикой новые задачи по выработке эффективных механизмов противодействия преступным посягательствам на информационную безопасность личности, общества и государства [13, с. 420]. Адекватное осмысление понятия и сущности компьютерной преступности имеет не только теоретическое, но и важное практическое значение, поскольку от правильного понимания природы данного феномена зависит эффективность мер по предупреждению, выявлению и пресечению соответствующих преступных деяний. Система компьютерной преступности представлена на рисунке 1.

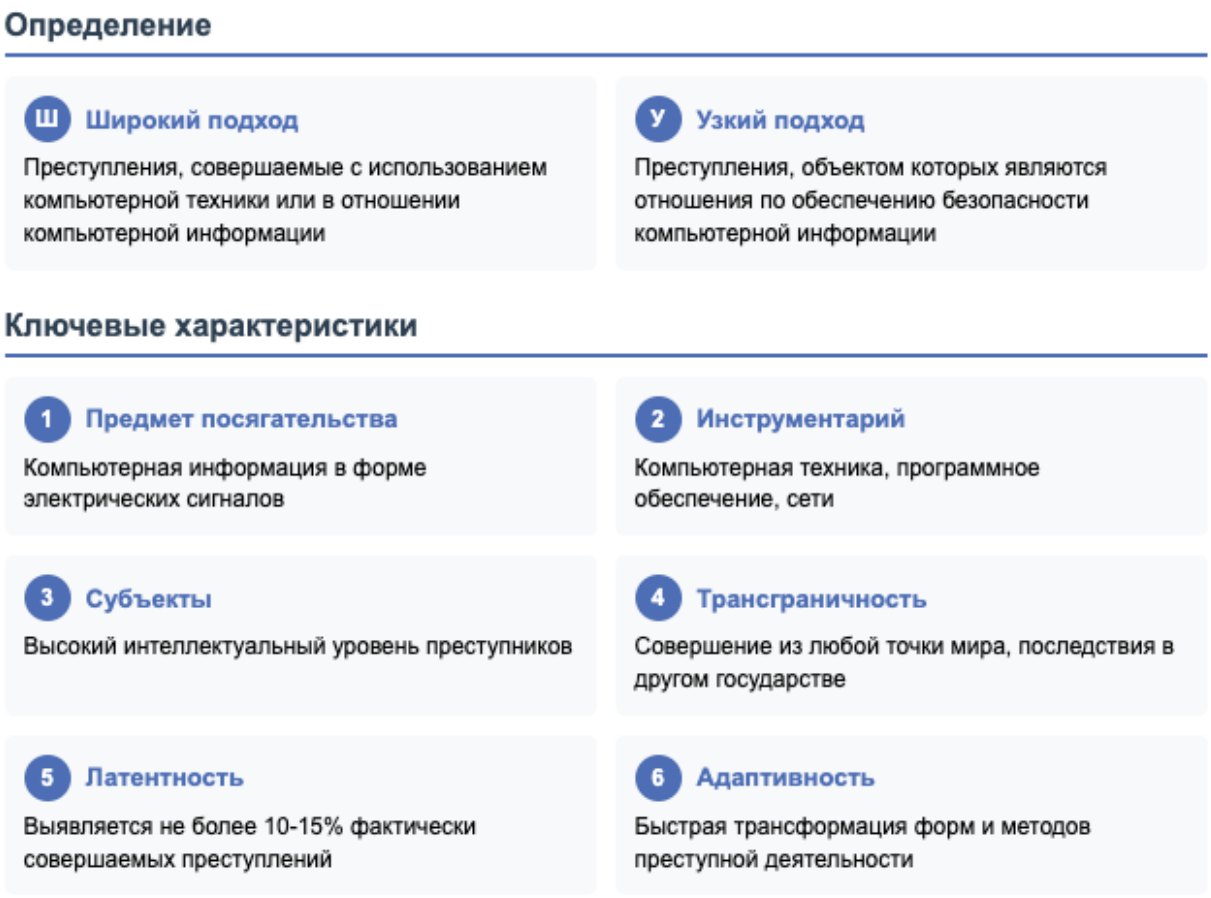


Рисунок 1 – Система компьютерной преступности

В научной доктрине уголовного права сформировался плюрализм концептуальных воззрений относительно сущностной характеристики компьютерной преступности. В контексте расширенной интерпретации

данное явление рассматривается как агрегация противозаконных действий, осуществляемых с использованием вычислительных систем либо направленных на цифровые данные и информационные экосистемы. Узкая трактовка определяет этот феномен как консолидацию уголовно-правовых деликтов, где непосредственным объектом посягательства выступают социальные отношения, обеспечивающие безопасность компьютерной информации и правомерное функционирование автоматизированных комплексов обработки данных [2, с. 126]. Именно последний подход послужил методологической основой для инкорпорации в Уголовный кодекс Российской Федерации специализированной главы 28 «Преступления в сфере компьютерной информации» [17, с. 46].

Необходимо акцентировать внимание на том, что в теоретическом дискурсе и международно-правовых актах синхронно с понятием «компьютерная преступность» используются альтернативные терминологические конструкции: «киберпреступность», «информационная преступность», «преступления в сфере высоких технологий», «преступления в сфере информационных технологий», что свидетельствует об отсутствии единообразного понятийного инструментария при описании рассматриваемого явления. При этом между обозначенными дефинициями прослеживаются фундаментальные смысловые дистинкции. В частности, концепт «киберпреступность» концентрируется на противоправных деяниях, реализуемых в киберпространстве – специфической среде, формируемой конвергентными информационно-телекоммуникационными сетями, и представляет собой более широкую категорию в сопоставлении с термином «компьютерная преступность». В то же время, понятие «информационная преступность» охватывает не только правонарушения, связанные с компьютерной информацией, но и иные противозаконные действия, посягающие на информационную безопасность, включая нелегальный оборот специальных технических средств для негласного получения информации, нарушение тайны переписки и телефонных переговоров и прочие.

Онтология компьютерной преступности как социально-правового феномена детерминируется комплексом имманентных характеристик, дифференцирующих данную форму противоправной активности от классических видов преступного поведения. Прежде всего, компьютерная преступность характеризуется специфичным предметом криминального посягательства – компьютерной информацией, которая согласно примечанию к ст. 272 УК РФ интерпретируется как сведения (сообщения, данные), представленные в формате электрических сигналов, вне зависимости от технических средств их сохранения, процессинга и трансляции [14, с. 489]. При этом компьютерная информация обладает рядом уникальных атрибутов, таких как нематериальная природа, потенциал существования в различных форматах (файлы, базы данных, программы и так далее), способность к дублированию без ущерба для оригинала, что кардинально влияет на механизмы осуществления противоправных действий и методологию их расследования [8, с. 538].

Другим значимым атрибутом компьютерной преступности выступает специфический инструментарий осуществления противоправных деяний – вычислительная техника, программное обеспечение, информационно-телекоммуникационные сети, которые могут функционировать как в качестве средства совершения преступления, так и в качестве его объекта или локации осуществления. При этом имплементация современных информационных технологий при реализации преступных замыслов предоставляет злоумышленникам инновационные возможности, такие как дистанционный доступ к объекту посягательства, обеспечение анонимности, автоматизация противоправных операций, что значительно осложняет детекцию и расследование данной категории преступлений.

Компьютерная преступность характеризуется также особой субъектной композицией. Если на начальных этапах эволюции компьютерных технологий субъектами соответствующих противоправных деяний выступали преимущественно индивиды, обладающие углубленными знаниями и

компетенциями в сфере программирования и информационных технологий (так называемые «хакеры»), то в современных условиях спектр потенциальных субъектов компьютерных преступлений существенно расширился. Это обусловлено как повышением общего уровня цифровой грамотности населения, так и появлением на нелегальных рынках готовых программных решений и сервисов, обеспечивающих возможность совершения противоправных деяний в информационной сфере без специализированных технических познаний [16, с. 98]. Вместе с тем, компьютерные преступления, особенно их комплексные модификации, по-прежнему характеризуются высоким интеллектуальным уровнем субъектов, что дифференцирует данную категорию преступности от общеуголовной.

Характерной особенностью компьютерной преступности является также ее трансграничная природа. В условиях глобализированного информационного пространства деликты в сфере компьютерной информации могут инициироваться из любой географической точки планеты, при этом юридически значимые последствия наступают на территории другого государства, что генерирует значительные сложности как для квалификации данных деяний, так и для привлечения виновных лиц к уголовной ответственности. Данное обстоятельство актуализирует необходимость международной кооперации в противодействии компьютерной преступности, гармонизации национальных правовых систем и разработки эффективных механизмов правовой помощи по уголовным делам рассматриваемой категории.

Компьютерная преступность характеризуется также высоким уровнем латентности, детерминированной как технической сложностью обнаружения и фиксации цифровых следов преступления, так и нежеланием потерпевших субъектов (особенно коммерческих структур) обращаться в правоохранительные органы из-за рисков репутационных потерь и разглашения конфиденциальной информации в процессе расследования. По экспертным оценкам, выявляется и документируется не более 10-15%

фактически совершаемых компьютерных преступлений, что осложняет объективную оценку реальных масштабов данного феномена и разработку адекватных превентивных механизмов [4, с. 46]. Исследования последних лет показывают, что латентность киберпреступности остается одной из ключевых проблем, препятствующих эффективному противодействию данному явлению [32, с. 78].

Существенной характеристикой компьютерной преступности является ее высокая адаптивность к изменяющимся условиям и способность к оперативной трансформации форм и методов криминальной активности. С появлением инновационных информационных технологий и сервисов формируются и новые модели их противоправного использования, что ставит перед законодателем задачу своевременной криминализации общественно опасных деяний в информационном пространстве. При этом эволюция нормативно-правовой базы в данной сфере неизбежно отстает от динамики развития компьютерной преступности, что создает определенные пробелы в уголовно-правовой защите информационной безопасности.

Сущность компьютерной преступности как социально-правового феномена проявляется также в ее интеграции с другими видами преступной деятельности. С одной стороны, цифровые технологии все активнее используются как инструментарий совершения традиционных преступлений (мошенничества, нарушения авторских прав, распространения порнографических материалов и так далее), с другой – компьютерные преступления зачастую выступают в качестве способа или этапа реализации более тяжких преступных посягательств, например, террористических акций, промышленного шпионажа, хищений в особо крупном размере. Данная тенденция свидетельствует о конвергенции различных типов преступности в условиях информационного общества и требует комплексного подхода к их предупреждению и нейтрализации.

В парадигме уголовно-правовой науки фундаментальную значимость приобретает проблематика классификации преступных посягательств,

конституирующих явление компьютерной преступности. В системе российского уголовного законодательства корпус преступлений в сфере компьютерной информации консолидирует противоправные деяния, регламентированные статьями 272-274.2 УК РФ: несанкционированный доступ к компьютерной информации (ст. 272), разработка, применение и диссеминация вредоносных компьютерных программ (ст. 273), несоблюдение регламента эксплуатации средств хранения, обработки или трансляции компьютерной информации и информационно-телекоммуникационных сетей (ст. 274), противоправное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1), нарушение нормативов централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети "Интернет" и сети связи общего пользования (ст. 274.2). Одновременно, при экстенсивном толковании феномен компьютерной преступности интегрирует также правонарушения, где компьютерные технологии выступают инструментальным средством их совершения, в частности, мошеннические действия с использованием электронных средств платежа (ст. 159.3 УК РФ), мошенничество в области компьютерной информации (ст. 159.6 УК РФ), посягательства на авторские и смежные права в отношении программного обеспечения и баз данных (ст. 146 УК РФ) и иные составы преступлений.

Общественная опасность компьютерной преступности детерминируется не только масштабом причиняемого материального ущерба, который согласно отдельным аналитическим оценкам достигает сотен миллиардов долларов ежегодно в глобальном измерении, но и иными негативными последствиями, такими как дестабилизация функционирования информационных систем, утрата контроля над критически важными элементами инфраструктуры, компрометация конфиденциальности персональных данных, дискредитация электронной коммерции и государственных цифровых сервисов. В условиях

цифровой трансформации экономики и государственного управления компьютерная преступность трансформируется в одну из приоритетных угроз национальной безопасности, требующую разработки и имплементации комплексных мер противодействия. Современные исследования подтверждают, что киберпреступность представляет комплексную угрозу, требующую интегрированного подхода к противодействию как на уровне уголовно-правовых, так и криминологических мер [25, с. 420].

Таким образом, понятие и сущность компьютерной преступности в обществе определяются совокупностью ее сущностных характеристик, включая особый предмет посягательства (компьютерную информацию), специфический инструментарий совершения преступлений (информационные технологии), особый субъектный состав, трансграничный характер, высокую латентность, адаптивность и взаимосвязь с другими видами преступности.

## 1.3 Понятие преступлений в сфере компьютерной информации, их особенности

В эпоху цифровой трансформации современного социума компьютерные технологии интегрировались практически во все домены человеческой активности, став фундаментальным элементом экономических, политических, социокультурных и институциональных процессов. Интенсивная эволюция информационно-коммуникационных технологий, параллельно с неоспоримыми позитивными эффектами, сгенерировала комплекс инновационных рисков, ассоциированных с потенциалом их имплементации в противоправных целях. В данном контексте особую значимость приобретает уголовно-правовая протекция общественных отношений, формирующихся в области обеспечения безопасности компьютерной информации и стабильного функционирования автоматизированных систем процессинга данных. Концептуализация дефиниции и специфических характеристик преступлений в сфере

компьютерной информации имеет фундаментальное теоретическое и прикладное значение для оптимизации механизмов уголовно-правового противодействия данной категории криминальных деяний [1, с. 128].

В теоретическом пространстве уголовного права сформировались многовариантные методологические концепции к определению сущности преступлений в сфере компьютерной информации. При рестриктивной трактовке данные преступления интерпретируются как закрепленные уголовным законодательством общественно опасные деяния, где непосредственным объектом посягательства выступают социальные отношения, обеспечивающие безопасность компьютерной информации и легитимное функционирование автоматизированных систем обработки данных. Эта теоретическая конструкция находится в конгруэнтности со структурной организацией Уголовного кодекса Российской Федерации, где выделен самостоятельный раздел - глава 28 «Преступления в сфере компьютерной информации», охватывающая статьи 272-274.2 УК РФ [1].

Дискуссия о содержании понятия преступлений против компьютерной информации ведется в научной литературе с момента введения соответствующих норм в УК РФ, при этом большинство исследователей выделяют специфику объекта и предмета данных преступлений как определяющий критерий [2, с. 126]. Законодатель при формировании данного структурного элемента исходил из постулата, что родовым объектом обозначенных преступлений являются общественные отношения, обеспечивающие общественную безопасность и порядок, а видовым объектом - социальные отношения, возникающие в процессе безопасного формирования, сохранения, процессинга и трансляции компьютерной информации [11, с. 48].

В контексте экстенсивной интерпретации к преступлениям в сфере компьютерной информации причисляют не только деяния, предусмотренные главой 28 УК РФ, но и иные криминальные посягательства, осуществляемые посредством компьютерной техники либо в отношении цифровой

информации, в частности, мошеннические действия в сфере компьютерной информации (ст. 159.6 УК РФ), нарушения авторских и смежных прав относительно программного обеспечения и информационных баз (ст. 146 УК РФ), противоправные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, с применением специальных технических средств (ст. 183 УК РФ) и другие. Такая методологическая позиция обеспечивает более полный охват всего диапазона преступных деяний, связанных с использованием информационных технологий, однако размывает концептуальные границы феномена преступлений в сфере компьютерной информации, что затрудняет его теоретическое осмысление и практическую реализацию.

Для конструирования точной дефиниции преступлений в сфере компьютерной информации необходимо установить их сущностные характеристики, отграничивающие данную категорию противоправных деяний от других уголовно наказуемых посягательств. Базовым и определяющим признаком выступает особый предмет преступного посягательства - компьютерная информация. Согласно примечанию к ст. 272 УК РФ под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, вне зависимости от способов их хранения, обработки и передачи. Данное легальное определение подчеркивает специфическую форму существования компьютерной информации - в виде электрических сигналов, что кардинально отличает ее от информации, зафиксированной на иных материальных носителях (бумажных документах, фотоматериалах и прочих).

Компьютерная информация характеризуется совокупностью специфических атрибутов, оказывающих существенное влияние на характер и модусы осуществления преступлений в рассматриваемой области. К таким атрибутам относятся: нематериальная природа (что затрудняет идентификацию факта ее хищения или уничтожения), потенциал существования в многообразных формах (файлы, программы, базы данных и

так далее), способность к дублированию без деградации оригинала, возможность дистанционного доступа и управления, комплексность обнаружения и документирования следов противоправных манипуляций. Указанные характеристики детерминируют особенности объективной стороны преступлений в сфере компьютерной информации, которые могут реализовываться удаленно, без непосредственного контакта с потерпевшим субъектом или объектом посягательства, а также с высокой интенсивностью и в масштабах, недоступных для традиционных видов криминальной активности.

Ключевой характеристикой киберпреступлений выступает их уникальный механизм реализации, неразрывно связанный с применением компьютерного оборудования и телекоммуникационных сетевых структур. Примечательно, что вычислительные системы могут выполнять дуалистическую функцию: выступать как операционный инструментарий криминальной деятельности (в частности, при разработке и диссеминации вредоносного программного обеспечения), так и становиться непосредственной мишенью противоправных действий (например, при дестабилизации регламентированных режимов эксплуатации информационно-вычислительных комплексов). В определенных обстоятельствах наблюдается конвергенция этих функциональных аспектов, когда правонарушитель задействует одну вычислительную платформу для несанкционированного проникновения в информационные массивы, размещенные на другом компьютерном устройстве [20, с. 220].

Фундаментальной характеристикой информационных преступлений является их целевая ориентация на компрометацию защищенности компьютерных данных и дезорганизацию штатного функционирования автоматизированных систем обработки информации. Данный атрибутивный признак манифестирует сущностные параметры видового объекта рассматриваемых преступлений и обеспечивает методологическую основу для их дифференциации от иных противоправных деяний, реализуемых с

использованием цифровых технологий, но направленных на нарушение других охраняемых уголовным законодательством общественных отношений (к примеру, незаконное присвоение денежных средств посредством электронных платежных инструментов).

На основании выявленных сущностных характеристик представляется возможным сформулировать следующее концептуальное определение: преступления в сфере компьютерной информации представляют собой криминализированные уголовным законодательством общественно опасные действия, направленные на нарушение информационной безопасности и дестабилизацию функционирования автоматизированных систем обработки данных, осуществляемые либо с применением вычислительной техники, либо в отношении цифровой информации [6, с. 67].

Архитектура компьютерных преступлений в российском уголовном праве, представлены на рисунке 2, интегрирует следующие составы: несанкционированный доступ к компьютерной информации (ст. 272 УК РФ), разработка, внедрение и распространение вредоносного программного обеспечения (ст. 273 УК РФ), нарушение эксплуатационных регламентов средств хранения, обработки или трансляции компьютерной информации и телекоммуникационных сетей (ст. 274 УК РФ), деструктивное воздействие на критическую информационную инфраструктуру РФ (ст. 274.1 УК РФ), нарушение правил централизованного администрирования технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования российского сегмента сети «Интернет» и телекоммуникационной сети общего пользования (ст. 274.2 УК РФ).

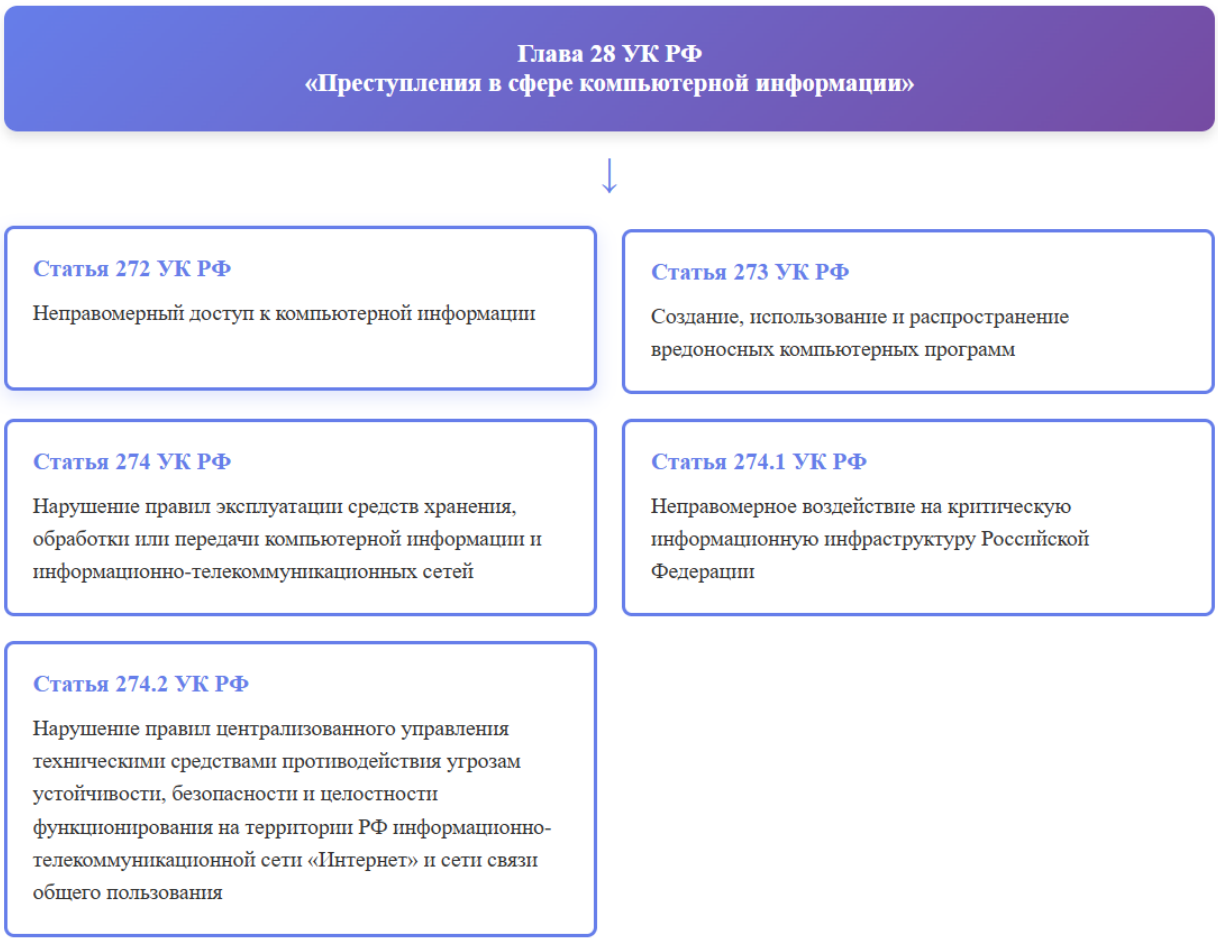


Рисунок 2 – Архитектура компьютерных преступлений в российском уголовном праве

Преступления в сфере компьютерной информации характеризуются комплексом особенностей, дифференцирующих их от классических видов преступных деяний и оказывающих существенное влияние на их квалификацию и процесс расследования.

Первичной такой особенностью является высокий уровень латентности данных преступлений, детерминированный как технической сложностью обнаружения и документирования цифровых следов, так и нежеланием потерпевших субъектов (особенно коммерческих организаций) инициировать обращение в правоохранительные структуры из-за рисков репутационных потерь и дискредитации конфиденциальной информации в процессе расследования. По экспертным оценкам, выявляется и документируется не более 10-15% фактически реализуемых компьютерных преступлений, что

существенно осложняет объективную оценку реальных параметров данного феномена и разработку адекватных механизмов противодействия [15, с. 62].

Второй особенностью преступлений в сфере компьютерной информации является их транснациональный характер. В условиях глобального информационного пространства данные преступления могут совершаться из любой точки мира, при этом последствия наступают в другом государстве, что создает значительные сложности как для квалификации данных деяний, так и для привлечения виновных к уголовной ответственности. Решение данной проблемы требует развития международного сотрудничества в сфере борьбы с компьютерной преступностью, гармонизации национальных законодательств и разработки эффективных механизмов правовой помощи по уголовным делам данной категории.

Третьей особенностью преступлений в сфере компьютерной информации является их высокая технологичность, требующая от субъектов их расследования специальных знаний и навыков в области информационных технологий, а также использования специальных технических средств и методов. В этой связи особую значимость приобретает подготовка квалифицированных кадров для правоохранительных органов, специализирующихся на расследовании компьютерных преступлений, а также развитие научно-методического обеспечения данной деятельности.

Четвертой особенностью преступлений в сфере компьютерной информации является сложность установления причинно-следственной связи между деянием и наступившими последствиями, а также определения размера причиненного ущерба. Это обусловлено как нематериальным характером компьютерной информации, так и многообразием форм вреда, который может быть причинен в результате преступных посягательств на ее безопасность (материальный ущерб, моральный вред, репутационные потери, угроза национальной безопасности и так далее). Данная особенность создает

определенные трудности при квалификации преступлений в сфере компьютерной информации и назначении наказания за их совершение.

Пятой особенностью преступлений в сфере компьютерной информации является их высокая общественная опасность, обусловленная возможностью причинения значительного вреда широкому кругу лиц с минимальными затратами ресурсов со стороны преступника. Так, распространение вредоносной программы может привести к нарушению работы множества компьютеров и информационных систем, причинив ущерб, исчисляемый миллионами долларов. При этом такие преступления могут иметь катастрофические последствия, если они направлены на объекты критической информационной инфраструктуры (системы управления транспортом, энергетическими и гидротехническими сооружениями, предприятиями ядерной энергетики и так далее).

Шестой особенностью преступлений в сфере компьютерной информации является их высокая динамичность и способность к трансформации форм и методов преступной деятельности в ответ на развитие технологий и систем защиты информации. Данная особенность требует от законодателя своевременной корректировки уголовно-правовых норм, направленных на противодействие компьютерной преступности, а также разработки гибких механизмов их применения, способных адаптироваться к изменяющимся условиям информационной среды.

Указанные особенности преступлений в сфере компьютерной информации оказывают существенное влияние на конструирование соответствующих составов преступлений в уголовном законодательстве. Так, при формулировании диспозиций статей 272-274.2 УК РФ законодатель использовал ряд специфических технических терминов (компьютерная информация, вредоносная программа, средства хранения, обработки или передачи компьютерной информации, информационно-телекоммуникационная сеть, критическая информационная инфраструктура и

та далее), которые требуют специального толкования с учетом положений информационного законодательства и достижений компьютерных наук.

Таким образом, понятие преступлений в сфере компьютерной информации охватывает совокупность предусмотренных уголовным законом общественно опасных деяний, посягающих на безопасность компьютерной информации и нормальное функционирование автоматизированных систем обработки данных, совершаемых с использованием средств компьютерной техники или в отношении компьютерной информации. Данные преступления характеризуются рядом особенностей, включая высокую латентность, транснациональный характер, технологичность, сложность установления причинно-следственной связи между деянием и последствиями, высокую общественную опасность и динамичность.

Подводя итоги первой главы, мы пришли к следующим выводам.

Анализ исторического развития законодательства показал поэтапное формирование правовой базы: от квалификации по общим составам преступлений до появления специальной главы в УК РФ 1996 года о преступлениях в сфере компьютерной информации.

Исследование выявило основные характеристики компьютерной преступности: высокую латентность, транснациональный характер, значительный ущерб и сложность расследования. Предложено авторское определение компьютерного преступления как общественно опасного деяния, совершаемого с использованием компьютерных технологий либо направленного на компьютерную информацию, посягающего на информационную безопасность.

Особенности компьютерных преступлений включают специфический предмет посягательства, особый механизм следообразования и возможность дистанционного совершения. Выявлена недостаточность существующего понятийного аппарата для описания всего многообразия преступлений в информационной сфере.

# Глава 2 Уголовно-правовая характеристика компьютерных преступлений

## 2.1 Объективные признаки компьютерных преступлений

Компьютерные преступления представляют собой одну из наиболее интенсивно эволюционирующих категорий криминальных деяний в условиях формирования глобального информационного социума. Объективные конститутивные признаки данной типологии преступных посягательств имеют детерминирующее значение для их корректной юридической квалификации в системе уголовно-правовых норм. В российском законодательном пространстве компьютерные преступления преимущественно кодифицированы в рамках главы 28 Уголовного кодекса Российской Федерации «Преступления в сфере компьютерной информации», однако дискретные составы преступлений, ассоциированные с использованием компьютерного инструментария, инкорпорированы также в иные структурные компоненты УК РФ. Настоящее научное исследование ориентировано на комплексную аналитическую экспликацию объективных признаков компьютерных преступлений с позиции их уголовно-правовой характеристики.

Объективные признаки преступления в доктринальном пространстве уголовного права традиционно интегрируют объект и объективную сторону криминального деяния [23, с. 50]. При аналитическом исследовании компьютерных преступлений необходимо осуществить детализированную экспертизу специфики указанных элементов состава преступления, принимая во внимание уникальные характеристики цифровой экосистемы, в которой реализуются данные противоправные акты. Объектом преступного посягательства выступают общественные отношения, находящиеся под протекцией уголовного закона, на которые направлено криминальное деяние. Объективная сторона характеризует экстернальное проявление преступного

акта и включает деяние (действие или бездействие), общественно опасные последствия, каузальную связь между деянием и последствиями, а также темпоральные, локационные, ситуационные характеристики, способ, орудия и средства реализации преступного замысла.

В структуре объектов компьютерных преступлений, кодифицированных в главе 28 УК РФ, родовым объектом выступают социальные отношения в области обеспечения компьютерной безопасности. Видовой объект охватывает отношения, обеспечивающие сохранность компьютерной информации и правомерную эксплуатацию компьютерных систем. Непосредственные объекты конкретных составов охватывают более узкие группы общественных отношений, включающие безопасность компьютерной информации, санкционированный доступ к ней, ее целостность и доступность, защищенность информационно-телекоммуникационных сетей и другие аспекты.

Уникальная характеристика компьютерных преступлений состоит в том, что объектом криминального посягательства преимущественно является компьютерная информация. В соответствии с примечанием к статье 272 УК РФ, компьютерная информация определяется как сведения (сообщения, данные), выраженные в форме электрических сигналов, вне зависимости от способов их хранения, обработки и трансляции. Компьютерная информация обладает рядом специфических свойств: нематериальная сущность, возможность копирования без физического изъятия, способность к мгновенной передаче на большие расстояния, что существенно влияет на особенности объективной стороны данных преступлений [30, с. 85].

Объективная сторона компьютерных преступлений характеризуется широким спектром действий, направленных на противоправное использование или деструктивное воздействие на компьютерную информацию. Статья 272 УК РФ криминализирует несанкционированный доступ к компьютерной информации, повлекший ее уничтожение, блокирование, модификацию или копирование. Объективная сторона данного

преступления реализуется посредством активных действий по получению доступа к компьютерной информации без разрешения правообладателя или в нарушение установленного порядка доступа.

Конструкция состава преступления по статье 272 УК РФ является материальной, требующей наступления последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации. Уничтожение информации подразумевает такое воздействие, при котором она перестает существовать для владельца и не поддается восстановлению стандартными или специальными программными средствами. Блокирование представляет собой создание условий, при которых легитимный пользователь полностью или частично утрачивает доступ к информации. Модификация означает внесение изменений в исходную информацию, результатом чего становится появление ее новой версии, отличной от первоначальной. Копирование заключается в создании идентичного экземпляра информации на другом носителе или в иной области того же носителя.

Ключевым элементом объективной стороны преступления по статье 272 УК РФ является установление причинно-следственной связи между несанкционированным доступом к компьютерной информации и наступившими последствиями. Для привлечения лица к уголовной ответственности требуется доказать, что именно его действия по неправомерному доступу обусловили уничтожение, блокирование, модификацию или копирование компьютерной информации.

Статья 273 УК РФ устанавливает ответственность за создание, использование и распространение вредоносных компьютерных программ. Объективная сторона данного преступления экстернализируется в форме действий по созданию, распространению или использованию компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Создание вредоносной программы предполагает ее разработку, программирование, подготовку к практическому использованию. Распространение вредоносной программы может осуществляться посредством ее трансляции другим субъектам, размещения в публичном доступе в информационно-телекоммуникационных сетях, массовой дистрибуции по электронной почте и альтернативными методами. Использование вредоносной программы означает ее практическую имплементацию для достижения целей, для которых она была спроектирована [37, с. 40].

Специфической характеристикой объективной стороны преступления, предусмотренного статьей 273 УК РФ, является то, что его состав сконструирован как формальный. Для квалификации деяния по данной статье не требуется наступления общественно опасных последствий — достаточно самого факта создания, распространения или использования вредоносной программы. Это обусловлено повышенной степенью общественной опасности таких действий и потенциальной вероятностью причинения значительного ущерба.

Статья 274 УК РФ предусматривает ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Объективная сторона данного преступления манифестируется в нарушении правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшем уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб [39, с. 76].

В отличие от преступления, предусмотренного статьей 272 УК РФ, в рассматриваемом случае речь идет о нарушении правил эксплуатации субъектом, обладающим легитимным доступом к компьютерной информации

и обязанным соблюдать установленные регламенты ее использования. Состав преступления по статье 274 УК РФ является материальным, поскольку для квалификации деяния необходима констатация последствий в виде уничтожения, блокирования, модификации либо копирования компьютерной информации, причинивших крупный ущерб.

В 2017 году Уголовный кодекс РФ был дополнен статьей 274.1, устанавливающей ответственность за неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации. Данная статья предусматривает ответственность за создание, распространение и использование компьютерных программ, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру, неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре, а также нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре.

Объективная сторона преступлений, предусмотренных статьей 274.1 УК РФ, демонстрирует структурную аналогию с объективной стороной преступлений, регламентированных статьями 272-274 УК РФ, но характеризуется определенной спецификой, детерминированной особым объектом посягательства - критической информационной инфраструктурой Российской Федерации. Под критической информационной инфраструктурой понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, функционирующие в сферах здравоохранения, науки, транспорта, связи, энергетики, банковской и финансовой сферах, топливно-энергетического комплекса, в области атомной энергии, оборонной, ракетно-космической, горнодобывающей, металлургической и химической промышленности.

Правовое регулирование защиты критической информационной инфраструктуры осуществляется специальным федеральным законом,

устанавливающим требования к обеспечению безопасности значимых объектов и порядок реагирования на компьютерные инциденты [34]. Законодательное выделение критической информационной инфраструктуры в качестве особого объекта уголовно-правовой охраны отражает современные тенденции развития института ответственности за компьютерные преступления [29, с. 98].

Помимо преступлений, кодифицированных в главе 28 УК РФ, к категории компьютерных преступлений могут быть отнесены и иные преступные деяния, реализуемые с использованием компьютерных технологий. Например, мошенничество в сфере компьютерной информации, ответственность за которое установлена статьей 159.6 УК РФ. Объективная сторона данного преступления манифестируется в хищении чужого имущества или приобретении права на чужое имущество посредством ввода, удаления, блокирования, модификации компьютерной информации либо иного вмешательства в функционирование средств хранения, обработки или передачи компьютерной информации или информационно-телекоммуникационных сетей. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, требует учета специфики способа совершения преступления и используемых технических средств [28, с. 112].

Специфика объективной стороны мошенничества в сфере компьютерной информации заключается в модусе совершения преступления, который предполагает использование компьютерных технологий для неправомерного завладения чужим имуществом или правами на него. Такое мошенничество может реализовываться различными методами, включая фишинг (создание фальсифицированных веб-ресурсов, имитирующих официальные сайты банков, платежных систем и других организаций), использование вредоносных программ для интерцепции конфиденциальной информации, несанкционированный доступ к банковским счетам и электронным платежным инструментам и так далее [35, с. 25].

К категории компьютерных преступлений также могут быть отнесены нарушения авторских и смежных прав (статья 146 УК РФ), реализуемые посредством незаконного использования компьютерных программ, баз данных и иных объектов авторского права в цифровом формате. Объективная сторона данного преступления может экстернализироваться в незаконном копировании и распространении программного обеспечения, цифрового контента, в том числе через информационно-телекоммуникационные сети.

Статья 138.1 УК РФ устанавливает ответственность за незаконный оборот специальных технических средств, предназначенных для негласного получения информации. Объективная сторона данного преступления может быть ассоциирована с распространением программного обеспечения, предназначенного для негласного получения компьютерной информации, например, программ-кейлоггеров, способных регистрировать нажатия клавиш на клавиатуре и транслировать эту информацию злоумышленнику [27, с. 183].

Статья 183 УК РФ предусматривает ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну. Объективная сторона данного преступления может манифестироваться в неправомерном доступе к компьютерным системам организаций с целью получения конфиденциальной информации, составляющей коммерческую или иную охраняемую законом тайну.

Существенную проблему при квалификации компьютерных преступлений представляет определение локации совершения преступления, поскольку виртуальное пространство не характеризуется четкими географическими демаркациями. Преступник, информационная система, на которую он осуществляет воздействие, и потерпевший могут находиться в различных юрисдикциях. В соответствии со статьей 11 УК РФ, лицо, совершившее преступление на территории Российской Федерации, подлежит уголовной ответственности по УК РФ. При этом преступление признается совершенным на территории РФ, если деяние было инициировано или продолжено или было завершено на территории Российской Федерации. В

контексте компьютерных преступлений это может означать, что если либо субъект преступления, либо потерпевший, либо информационная система, на которую было направлено преступное воздействие, локализовались на территории России, то преступление квалифицируется как совершенное на территории Российской Федерации.

Значимым аспектом объективной стороны компьютерных преступлений является использование специфического инструментария совершения преступления. В качестве такого инструментария могут выступать как аппаратные средства (компьютеры, серверы, мобильные устройства), так и программные компоненты (вредоносные программы, эксплойты, утилиты для взлома аутентификационных данных и так далее). Специфика данного инструментария оказывает существенное влияние на модус совершения преступления и его юридическую квалификацию.

Характерной особенностью компьютерных преступлений является то, что они часто реализуются дистанционно, без непосредственного физического контакта преступника с потерпевшим или объектом преступного посягательства. Это генерирует дополнительные методологические сложности при расследовании таких преступлений и установлении всех обстоятельств, интегрированных в предмет доказывания.

При аналитическом исследовании объективных признаков компьютерных преступлений необходимо принимать во внимание, что эволюция информационных технологий детерминирует появление инновационных форм общественно опасных деяний, которые могут не охватываться существующими составами преступлений. В связи с этим актуализируется необходимость в перманентном совершенствовании уголовного законодательства в сфере противодействия компьютерным преступлениям.

В заключение следует отметить, что объективные признаки компьютерных преступлений характеризуются определенной спецификой, обусловленной особенностями информационного пространства как среды

совершения преступления. Эта специфика проявляется в особенностях объекта и предмета преступления, характере общественно опасного деяния, его последствиях, особенностях причинно-следственной связи, а также времени, места, обстановки, способа, орудий и средств совершения преступления. Правильное установление и оценка объективных признаков компьютерных преступлений имеет решающее значение для их правильной квалификации и эффективного применения мер уголовно-правового воздействия в отношении лиц, совершающих такие преступления.

## 2.2 Субъективные признаки компьютерных преступлений

Субъективные признаки компьютерных преступлений конституируют комплексную систему характеристик, репрезентирующих внутреннюю, психическую детерминацию индивида к осуществляемому им социально деструктивному деянию в области компьютерной информации и его результативным проявлениям. В соответствии с классической парадигмой структурирования состава преступления в уголовно-правовой доктрине субъективные признаки интегрируют два фундаментальных компонента: субъективную сторону преступного акта и субъекта криминального посягательства. Многоаспектная экспликация данных элементов применительно к компьютерным преступлениям обладает существенной сигнификативностью для адекватной квалификации деяний, демаркации смежных составов преступлений и имплементации принципа справедливости при определении пенализационных мер [40, с. 25].

Субъективная сторона компьютерных преступлений дескриптируется посредством таких дифференцирующих атрибутов, как вина, мотивационные императивы, целевые ориентации и эмоционально-психологическое состояние индивида в момент операционализации преступного акта. Вина конституирует облигаторный признак субъективной стороны любого криминального деяния, включая и компьютерное. В соответствии со

статьей 24 Уголовного кодекса Российской Федерации виновным в преступлении признается лицо, осуществившее деяние с умышленной интенциональностью или по неосторожности. При этом согласно части 2 указанной статьи деяние, реализованное по неосторожности, квалифицируется как преступление исключительно в тех случаях, когда это эксплицитно предусмотрено соответствующей статьей Особенной части УК РФ.

Детальное изучение криминальных составов, интегрированных в главу 28 УК РФ "Преступления в сфере компьютерной информации", приводит к фундаментальному заключению о преимущественно умышленном характере субъективной стороны данных противоправных деяний. В структуре умысла как формы вины законодатель дифференцирует прямой и косвенный варианты. Согласно нормативным положениям части 2 статьи 25 УК РФ, криминальное деяние квалифицируется как совершенное с прямым умыслом при наличии следующей триады признаков: осознание субъектом общественной опасности своего поведения, антиципация вероятности или неотвратимости наступления общественно опасных последствий и волевая направленность на их реализацию [36, с. 200]. Альтернативно, деяние классифицируется как совершенное с косвенным умыслом при осознании субъектом общественной опасности своих действий (бездействия), прогнозировании возможности наступления общественно опасных последствий при отсутствии прямого желания их наступления, но при сознательном допущении или безразличном отношении к ним.

При юридическом анализе состава преступления, предусмотренного статьей 272 УК РФ «Неправомерный доступ к компьютерной информации», принципиально важно отметить, что психическое отношение субъекта к совершаемому деянию может характеризоваться как прямым, так и косвенным умыслом. В ситуации прямого умысла правонарушитель обладает полным осознанием общественной опасности своих действий по несанкционированному доступу к информационным ресурсам, прогнозирует

вероятность или неизбежность наступления деструктивных последствий в форме уничтожения, блокирования, модификации или копирования информации и стремится к их реализации. При косвенном умысле субъект осознает противоправный характер своих действий, предвидит возможность наступления указанных последствий, но не имеет прямой заинтересованности в их наступлении, хотя сознательно допускает такую возможность или проявляет индифферентность.

Фундаментальным критерием при квалификации противоправного деяния по статье 272 УК РФ выступает верификация осознания субъектом неправомерности осуществляемого доступа к компьютерной информации. Данный аспект предполагает понимание лицом отсутствия легитимных оснований для доступа к информационным ресурсам или осознание факта нарушения установленного порядка доступа. В случае добросовестного заблуждения относительно правомерности доступа к информации, в действиях субъекта отсутствует умышленная составляющая, необходимая для квалификации по статье 272 УК РФ.

Психологическая составляющая преступления, регламентированного статьей 273 УК РФ «Создание, использование и распространение вредоносных компьютерных программ», характеризуется исключительно прямым умыслом. Правонарушитель демонстрирует полное осознание общественной опасности действий по разработке, распространению или применению вредоносного программного обеспечения или иной компьютерной информации и проявляет целенаправленное стремление к их осуществлению. Определяющим компонентом субъективной стороны выступает осознанное понимание субъектом того факта, что создаваемые, распространяемые или используемые им программные продукты или информационные массивы заведомо предназначены для несанкционированного уничтожения, блокирования, модификации, копирования информации или преодоления механизмов информационной защиты.

На это указывает использование в диспозиции статьи 273 УК РФ термина «заведомо», который имплицирует достоверное знание лицом определенных обстоятельств. Таким образом, для инициации процедуры привлечения к уголовной ответственности по данной статье необходимо верифицировать, что лицо осознавало деструктивный характер программы или информации, с которой оно осуществляло указанные в статье действия. Если лицо не осознавало вредоносного характера программы, например, полагая, что распространяет легитимное программное обеспечение, в его действиях отсутствует состав преступления, предусмотренного статьей 273 УК РФ.

Субъективная сторона преступления, регламентированного статьей 274 УК РФ «Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей», характеризуется виной в форме умысла или неосторожности. Это единственный состав в главе 28 УК РФ, который может быть совершен по неосторожности. Неосторожная форма вины в соответствии со статьей 26 УК РФ экспликируется в легкомыслии или небрежности. При легкомыслии лицо предвидит возможность наступления общественно опасных последствий своих действий (бездействия), но без достаточных к тому оснований самонадеянно рассчитывает на предотвращение этих последствий. При небрежности лицо не предвидит возможности наступления общественно опасных последствий своих действий (бездействия), хотя при необходимой внимательности и предусмотрительности должно было и могло предвидеть эти последствия [31, с. 260].

Общие положения о формах вины, закрепленные в статьях 25-26 УК РФ, применяются и при квалификации компьютерных преступлений, что подтверждается как доктринальными источниками, так и правоприменительной практикой [24, с. 234].

В контексте статьи 274 УК РФ неосторожность может манифестироваться, например, в том, что лицо, ответственное за

эксплуатацию компьютерных систем, не имплементирует требования по защите информации, полагая, что это не приведет к негативным последствиям, либо не предвидит возможности уничтожения или модификации компьютерной информации в результате своих действий, хотя должно было и могло это предвидеть в силу своих профессиональных обязанностей.

Особого внимания заслуживает субъективная сторона преступления, регламентированного статьей 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации». Данная статья была интегрирована в Уголовный кодекс Федеральным законом от 26.07.2017 № 194-ФЗ и устанавливает ответственность за различные формы неправомерного воздействия на объекты критической информационной инфраструктуры. Субъективная сторона данного преступления характеризуется виной в форме умысла, причем для квалификации по части 1 статьи 274.1 УК РФ требуется прямой умысел, на что указывает использование в диспозиции термина «заведомо».

Мотивационные императивы и целевые ориентации компьютерных преступлений могут быть дифференцированы и в большинстве случаев не конституируют облигаторные признаки субъективной стороны, за исключением квалифицированных составов. Так, часть 2 статьи 272 УК РФ устанавливает усиленную ответственность за неправомерный доступ к компьютерной информации, совершенный из корыстной заинтересованности. В данном случае корыстная заинтересованность выступает в качестве облигаторного признака субъективной стороны преступления и имплицирует интенцию лица получить материальную выгоду либо избежать материальных затрат.

Судебная практика, обобщенная в Постановлении Пленума Верховного Суда РФ от 30.11.2017 № 48, уточняет понимание корыстного мотива при квалификации преступлений, что имеет значение и для применения норм о компьютерных преступлениях [22].

Среди наиболее распространенных мотивационных императивов совершения компьютерных преступлений можно идентифицировать корыстные мотивы, реваншизм, хулиганские побуждения, желание продемонстрировать свои профессиональные компетенции, политические или идеологические детерминанты. В отдельных случаях мотивом может выступать так называемый кибер-вандализм, когда лицо стремится причинить деструктивное воздействие информационным системам или данным без какой-либо конкретной целевой ориентации. При этом установление мотива и цели преступления, даже если они не являются облигаторными признаками состава, имеет существенное значение для индивидуализации наказания и может учитываться судом при его определении.

Целевыми ориентациями совершения компьютерных преступлений могут быть получение конфиденциальной информации, дисфункционализация компьютерных систем, причинение имущественного ущерба, шпионаж, терроризм и другие. В отдельных случаях целевая ориентация преступления может индицировать наличие совокупности преступлений. Например, если неправомерный доступ к компьютерной информации осуществляется с целью последующего использования полученных данных для мошенничества, то действия виновного могут быть квалифицированы по статье 272 УК РФ и соответствующей части статьи 159 УК РФ.

Эмоционально-психологическое состояние лица в момент совершения компьютерного преступления редко обладает юридической сигнификативностью для квалификации деяния, однако может учитываться при определении наказания в качестве обстоятельства, характеризующего личность виновного.

Переходя к аналитической экспликации второго элемента субъективных признаков компьютерных преступлений - субъекта преступления, необходимо акцентировать внимание на том, что в большинстве случаев субъектом компьютерных преступлений является физическое вменяемое лицо,

достигшее возраста 16 лет. В соответствии со статьей 20 УК РФ за преступления, предусмотренные статьями 272-274.1 УК РФ, уголовная ответственность наступает с 16-летнего возраста. Редукция возраста уголовной ответственности до 14 лет за эти преступления законодателем не предусмотрена, несмотря на то, что в современном социуме подростки зачастую обладают высоким уровнем компьютерной грамотности и технически способны осуществлять компьютерные преступления.

Субъект преступления, регламентированного статьей 272 УК РФ, является общим, то есть им может быть любое лицо, достигшее 16-летнего возраста и соответствующее признакам, указанным в статье 19 УК РФ. При этом для квалификации деяния по части 3 статьи 272 УК РФ, устанавливающей ответственность за неправомерный доступ к компьютерной информации, совершенный лицом с использованием своего служебного положения, субъект преступления трансформируется в специальный. В данном случае речь идет о лице, которое в силу своего служебного положения обладает доступом к компьютерной информации или определенными полномочиями в отношении компьютерных систем и использует эти возможности для совершения преступления.

Аналогичная ситуация наблюдается и в отношении субъекта преступления, регламентированного статьей 273 УК РФ. В общем случае субъект данного преступления является общим, однако часть 2 статьи 273 УК РФ устанавливает усиленную ответственность за деяния, предусмотренные частью первой данной статьи, совершенные группой лиц по предварительному сговору или лицом с использованием своего служебного положения. В последнем случае субъект преступления также трансформируется в специальный [38, с. 210].

Особого внимания заслуживает субъект преступления, регламентированного статьей 274 УК РФ. В отличие от статей 272 и 273 УК РФ, субъект данного преступления изначально является специальным - им может быть только лицо, на которое возложена обязанность по соблюдению

правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, а также правил доступа к информационно-телекоммуникационным сетям. Такие обязанности могут быть возложены на лицо в силу его должностного положения, трудовых функций, договорных обязательств или иных оснований.

Специальным является и субъект преступления, регламентированного частью 3 статьи 274.1 УК РФ, устанавливающей ответственность за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации. Субъектом данного преступления может быть только лицо, обязанное соблюдать указанные правила.

В контексте аналитической экспликации субъекта компьютерных преступлений необходимо акцентировать внимание на проблеме идентификации личности преступника в условиях анонимизации, которую может обеспечивать интернет-пространство. Использование технологий анонимизации, таких как VPN, прокси-серверы, Tor и других, может существенно осложнить идентификацию лица, совершившего компьютерное преступление. Однако эти технические сложности не влияют на субъективные признаки преступления с точки зрения уголовного права - они лишь создают методологические трудности для правоприменительной практики при верификации факта совершения преступления конкретным лицом.

Существенным аспектом при аналитической экспликации субъективных признаков компьютерных преступлений является проблема вменяемости и ограниченной вменяемости. В соответствии со статьей 21 УК РФ не подлежит уголовной ответственности лицо, которое во время совершения общественно опасного деяния находилось в состоянии невменяемости, то есть не могло осознавать фактический характер и общественную опасность своих действий (бездействия) либо руководить ими вследствие хронического психического

расстройства, временного психического расстройства, слабоумия либо иного болезненного состояния психики.

Статья 22 УК РФ предусматривает, что вменяемое лицо, которое во время совершения преступления в силу психического расстройства не могло в полной мере осознавать фактический характер и общественную опасность своих действий (бездействия) либо руководить ими, подлежит уголовной ответственности. Однако психическое расстройство, не исключающее вменяемости, учитывается судом при определении наказания и может служить основанием для назначения принудительных мер медицинского характера.

В контексте компьютерных преступлений проблема вменяемости может иметь особую сигнификативность в связи с феноменом так называемой компьютерной зависимости или игровой аддикции, которая в отдельных случаях может достигать степени психического расстройства. В судебной практике известны прецеденты, когда защита пыталась использовать аргумент о наличии у обвиняемого компьютерной зависимости для смягчения его ответственности. Однако в большинстве случаев суды не признают компьютерную зависимость основанием для признания лица невменяемым или ограниченно вменяемым, если отсутствуют медицинские критерии невменяемости, установленные статьей 21 УК РФ.

При аналитической экспликации субъективных признаков компьютерных преступлений необходимо также акцентировать внимание на особенностях уголовной ответственности юридических лиц. В настоящее время в российском уголовном праве действует принцип персональной ответственности, согласно которому субъектом преступления может быть исключительно физическое лицо. Юридические лица не могут быть субъектами преступления и не подлежат уголовной ответственности. Однако в некоторых зарубежных юрисдикциях предусмотрена уголовная ответственность юридических лиц за определенные типологии преступлений, в том числе и компьютерные [21, с. 57].

В условиях глобализации и интеграции России в международное правовое пространство вопрос о введении уголовной ответственности юридических лиц периодически становится предметом научных дискуссий. Сторонники данной концепции указывают на то, что многие компьютерные преступления могут совершаться в интересах и с использованием ресурсного потенциала юридических лиц, что актуализирует вопрос о привлечении к ответственности не только конкретных физических лиц, но и организационных структур. Однако в настоящее время российское уголовное законодательство не предусматривает такой возможности, и юридические лица могут нести лишь административную или гражданско-правовую ответственность за правонарушения в сфере компьютерной информации.

Особого внимания заслуживает вопрос о субъективных признаках компьютерных преступлений, совершаемых в соучастии. В соответствии со статьей 32 УК РФ соучастием в преступлении признается умышленное совместное участие двух или более лиц в совершении умышленного преступления. Формы соучастия детерминированы в статье 35 УК РФ и включают группу лиц, группу лиц по предварительному сговору, организованную группу и преступное сообщество (преступную организацию).

Применительно к компьютерным преступлениям соучастие может манифестироваться в различных формах. Наиболее распространенной формой является группа лиц по предварительному сговору, когда два или более лица заблаговременно договариваются о совместном совершении преступления. Например, один соучастник может обеспечивать неправомерный доступ к компьютерной информации, а другой — использовать полученную информацию для совершения иных преступлений.

Более опасной формой соучастия является организованная группа, которая характеризуется устойчивостью, наличием организатора и заблаговременно разработанного плана преступной деятельности. В сфере компьютерных преступлений организованные группы могут специализироваться на различных видах криминальной активности, таких как

распространение вредоносных программ, неправомерный доступ к банковской информации, создание и использование фишинговых сайтов и так далее. [26].

Наиболее опасной формой соучастия является преступное сообщество (преступная организация), создаваемое для совершения тяжких или особо тяжких преступлений. В сфере компьютерных преступлений преступные сообщества могут иметь транснациональный характер и использовать сложные схемы легализации криминальных доходов. Необходимо акцентировать внимание на том, что в соответствии с частью 5 статьи 35 УК РФ лицо, создавшее организованную группу или преступное сообщество (преступную организацию) либо руководившее ими, подлежит уголовной ответственности за их организацию и руководство ими в случаях, предусмотренных статьями 205.4, 208, 209, 210 и 282.1 УК РФ, а также за все совершенные организованной группой или преступным сообществом (преступной организацией) преступления, если они охватывались его умыслом.

В заключение аналитической экспликации субъективных признаков компьютерных преступлений необходимо акцентировать внимание на том, что точная верификация формы вины, мотивационных императивов и целевых ориентаций преступления, а также идентификация субъекта преступления имеет детерминирующее значение для корректной квалификации деяния и определения справедливого наказания. Специфические особенности субъективных признаков компьютерных преступлений обусловлены уникальностью информационного пространства как среды совершения преступления, а также особым характером компьютерной информации как предмета криминального посягательства.

Эволюционная трансформация информационных технологий детерминирует появление инновационных форм общественно опасных деяний, что требует перманентного совершенствования уголовного законодательства и правоприменительной практики в сфере противодействия

компьютерным преступлениям. При этом особое внимание должно уделяться субъективным признакам преступлений, поскольку именно они позволяют дифференцировать преднамеренные преступные действия от ошибочных или неосторожных действий, которые могут не образовывать состава преступления или образовывать состав с меньшей степенью общественной опасности.

В данной главе реализован детализированный анализ объективных и субъективных признаков компьютерных преступлений, что позволяет сформировать целостную концептуальную модель уголовно-правовой характеристики данной типологии противоправных деяний.

Объективные признаки компьютерных преступлений обладают существенной спецификой, детерминированной особенностями информационного пространства как среды осуществления преступления. Родовым объектом таких преступлений являются общественные отношения в сфере обеспечения компьютерной безопасности, а предметом криминального посягательства выступает компьютерная информация, характеризующаяся уникальными атрибутами (нематериальность, возможность копирования без изъятия, дистанционный доступ).

Объективная сторона компьютерных преступлений экспликируется в многообразных деяниях, ориентированных на неправомерное использование компьютерной информации или деструктивное воздействие на нее. Большинство составов сконструированы как материальные, требующие наступления последствий в виде уничтожения, блокирования, модификации или копирования компьютерной информации. Специфическими характеристиками объективной стороны являются дистанционный характер совершения преступлений, использование специализированных технических и программных средств, а также методологическая сложность установления локации преступления.

Субъективные признаки компьютерных преступлений интегрируют субъективную сторону и субъекта преступления. Субъективная сторона

большинства компьютерных преступлений характеризуется умышленной формой вины (прямой или косвенный умысел), хотя в отдельных случаях, например, при нарушении правил эксплуатации средств хранения информации, возможна и неосторожная форма вины. Мотивационные императивы и целевые ориентации могут быть дифференцированы (корыстные, хулиганские, политические), и в ряде случаев являются квалифицирующими признаками.

Субъектом компьютерных преступлений в большинстве случаев является физическое вменяемое лицо, достигшее 16-летнего возраста. При этом для некоторых составов (например, нарушения правил эксплуатации средств хранения информации) субъект является специальным - лицом, на которое возложены соответствующие обязанности.

Особую сигнификативность имеет анализ компьютерных преступлений, совершаемых в соучастии, которые могут манифестироваться в различных формах (от группы лиц по предварительному сговору до транснациональных преступных сообществ).

Точная верификация всех объективных и субъективных признаков имеет детерминирующее значение для корректной квалификации компьютерных преступлений, демаркации смежных составов и определения справедливого наказания. Динамичная эволюция информационных технологий требует перманентного совершенствования уголовного законодательства и правоприменительной практики в данной сфере.

## 2.3 Квалифицирующие признаки преступлений в сфере компьютерной информации

Преступления в сфере компьютерной информации представляют собой относительно новую категорию уголовно наказуемых деяний, обусловленную стремительным развитием информационных технологий. Российское уголовное законодательство выделяет данную группу преступлений в

отдельную главу 28 УК РФ, что подчеркивает их специфический характер и особую общественную опасность. Действующая редакция Уголовного кодекса РФ содержит пять составов преступлений в сфере компьютерной информации (статьи 272-274.2), которые регулярно совершенствуются с учетом развития информационных технологий и правоприменительной практики [33].

Квалифицирующие признаки преступлений в сфере компьютерной информации имеют существенное значение для правоприменительной практики, поскольку они не только указывают на повышенную общественную опасность деяния, но и влияют на определение меры наказания. Данные признаки законодатель дифференцирует в зависимости от характера и степени общественной опасности конкретного преступления.

В составе неправомерного доступа к компьютерной информации (ч. 3 ст. 272 УК РФ от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) квалифицирующими признаками выступают:

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

Данные обстоятельства существенно повышают общественную опасность преступления, поскольку групповой характер преступления упрощает преодоление средств защиты информации, а использование служебного положения свидетельствует о нарушении дополнительных обязательств виновного лица.

В статье 273 УК РФ, устанавливающей ответственность за создание, использование и распространение вредоносных компьютерных программ, законодатель выделяет аналогичные квалифицирующие признаки: совершение деяния группой лиц по предварительному сговору, лицом с использованием своего служебного положения, а также наступление тяжких последствий или создание угрозы их наступления.

Наиболее детально квалифицирующие признаки разработаны для нарушения правил эксплуатации средств хранения, обработки или передачи

компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК РФ). Помимо традиционных квалифицирующих признаков, связанных с наступлением тяжких последствий, законодатель в 2017 году дополнил данную статью специальным составом (274.1 УК РФ), установив повышенную ответственность за нарушение правил эксплуатации критической информационной инфраструктуры Российской Федерации.

Нельзя не отметить, что в преступлениях в сфере компьютерной информации квалифицирующие признаки часто связаны с масштабом причиняемого ущерба, что обусловлено спецификой объекта преступления. Компьютерная информация может имать ключевое значение для функционирования финансовых институтов, органов государственной власти, транспортной инфраструктуры. Несанкционированное вмешательство в такие системы может привести к катастрофическим последствиям, что обосновывает введение особо квалифицирующих признаков, связанных с тяжкими последствиями.

Особенностью квалифицирующих признаков преступлений в сфере компьютерной информации является их преимущественно формально-материальный характер. Большинство составов сконструированы таким образом, что ответственность наступает уже за сам факт неправомерного доступа, создания вредоносных программ или нарушения правил эксплуатации, а наступление конкретных последствий выступает в качестве квалифицирующего признака, существенно повышающего наказание.

Следует отметить сложность выявления и доказывания некоторых квалифицирующих признаков в данной категории дел. Анализ актуальной судебной практики по делам о компьютерных преступлениях позволяет выявить характерные тенденции в применении норм уголовного законодательства в данной сфере и определить эффективность мер противодействия подобным правонарушениям.

Показательным примером является уголовное дело в отношении Николашкиной А.И., обвиняемой в совершении пяти преступлений,

предусмотренных ч. 3 ст. 272 УК РФ. Согласно материалам дела, подсудимая, работая в должности специалиста, а затем менеджера офиса продаж и обслуживания телекоммуникационной компании, неоднократно совершала неправомерный доступ к охраняемой законом компьютерной информации из корыстной заинтересованности с использованием своего служебного положения. Особенностью данного дела является квалификация действий по ч. 3 ст. 272 УК РФ с акцентом на использование служебного положения как квалифицирующий признак. Суд установил, что подсудимая, имея легальный доступ к базам данных в силу своих должностных обязанностей, осуществляла несанкционированные действия за пределами своих полномочий, четко определенных корпоративными инструкциями по безопасности. Данный пример демонстрирует тенденцию к более строгому подходу судов к оценке действий сотрудников, имеющих легитимный доступ к информационным системам, но превышающих свои полномочия.

Другим характерным примером является апелляционное постановление Московского городского суда от 25 ноября 2013 г. по делу № 10-11502/2013, касающееся осуждения группы лиц по ч. 2 ст. 272 УК РФ за проведение DDoS-атаки на информационные ресурсы коммерческой организации. Особый интерес представляет правовая позиция суда относительно трактовки понятия "неправомерный доступ к компьютерной информации" в контексте DDoS-атак. Суд отклонил доводы защиты о том, что в результате атаки не произошло непосредственного доступа к защищенной информации, указав, что блокирование работы системы электронной продажи билетов и нарушение нормального функционирования платежной системы квалифицируется как неправомерный доступ. Данное решение формирует важный прецедент, расширяющий толкование объективной стороны преступления, предусмотренного ст. 272 УК РФ, и демонстрирует адаптацию судебной практики к новым формам компьютерных преступлений.

Анализ этих судебных решений свидетельствует о формировании устойчивого подхода к квалификации компьютерных преступлений с учетом

современных технологических реалий. Суды придают особое значение субъективной стороне преступления, тщательно исследуя мотивы (в особенности корыстную заинтересованность), а также уделяют внимание техническим аспектам совершения деяния, привлекая для этого профильных экспертов. Отмечается тенденция к назначению реальных сроков лишения свободы за компьютерные преступления, особенно совершенные группой лиц или с использованием служебного положения, что отражает понимание судами высокой общественной опасности данной категории деяний.

В 2021 году законодатель внес дополнения в статьи главы 28 УК РФ, расширив перечень квалифицирующих признаков и уточнив содержание уже существующих. Поправки ужесточили ответственность за преступления в сфере компьютерной информации, совершенные в отношении критической информационной инфраструктуры Российской Федерации.

Квалифицирующие признаки преступлений в сфере компьютерной информации обладают определенной спецификой, связанной с особенностями объекта и предмета посягательства. Это подтверждается практикой Верховного Суда РФ, в частности, определением Судебной коллегии по уголовным делам № 5-КГ21-149-К2, где подробно рассматривается вопрос квалификации действий обвиняемых при неправомерном доступе к банковской информационной системе, повлекшем тяжкие последствия. Законодателю предстоит дальнейшее совершенствование данного института с учетом стремительного развития информационных технологий и появления новых общественно опасных моделей поведения в киберпространстве. В 2023 году в апелляционном определении Нижегородского областного суда по делу № 22-3156/2023 впервые был рассмотрен вопрос о квалификации DDoS-атаки на региональную медицинскую информационную систему как действия, создающего угрозу жизни людей, что подтверждает необходимость дальнейшей детализации квалифицирующих признаков в данной сфере.

Подводя итоги исследования главы 2, мы пришли к выводу, что комплексный анализ объективных признаков компьютерных преступлений

демонстрирует ярко выраженную специфику данной категории деяний, обусловленную особой природой цифрового пространства.

Родовым объектом рассматриваемых преступлений выступают общественные отношения в сфере обеспечения компьютерной безопасности.

Видовым объектом выступают отношения, обеспечивающие безопасность компьютерной информации и правомерное использование компьютерных систем.

Непосредственными объектами конкретных составов преступлений являются более узкие группы общественных отношений, таких как безопасность компьютерной информации, правомерный доступ к компьютерной информации, целостность и доступность компьютерной информации, безопасность информационно-телекоммуникационных сетей и так далее.

Предметом преступного посягательства служит компьютерная информация, обладающая уникальными свойствами: нематериальностью,

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

Субъективные признаки компьютерных преступлений характеризуются преимущественно умышленной формой вины (прямой или косвенный умысел), за исключением нарушения правил эксплуатации средств хранения информации, где допустима и неосторожная форма вины. Мотивационная сфера этих преступлений отличается многообразием (корыстные, хулиганские, политические мотивы), что в ряде случаев выступает квалифицирующим признаком.

Субъектом в большинстве составов является физическое вменяемое лицо, достигшее 16-летнего возраста, хотя для некоторых составов преступлений законодатель устанавливает специальный субъект.

Квалифицирующие признаки преступлений в сфере компьютерной информации обнаруживают определенную системность. Типичными квалифицирующими обстоятельствами выступают совершение деяния группой лиц по предварительному сговору или организованной группой.

Проведенный анализ в исследовании также выявил проблемы квалификации новых форм киберпреступлений (фишинг, кибersталкинг, DDoS-атаки), которые часто не имеют прямого отражения в уголовном законодательстве и квалифицируются по общим составам преступлений. Это указывает на необходимость совершенствования уголовного законодательства в данной сфере.

Таким образом, уголовно-правовая характеристика компьютерных преступлений представляет собой динамично развивающийся институт уголовного права, требующий постоянного научного осмысления и нормативного совершенствования с учетом трансформации цифровой среды и появления новых форм общественно опасного поведения в информационном пространстве.

## Глава 3 Организация и система мер противодействия компьютерной преступности

Стремительное развитие информационных технологий и цифровизация всех сфер жизни общества, наряду с очевидными преимуществами, привели к формированию принципиально нового вида преступности – компьютерной. Противодействие данному феномену представляет собой сложную комплексную задачу, требующую системного подхода, объединяющего правовые, организационные, технические и образовательные меры. В настоящей главе представлен анализ существующей системы противодействия компьютерной преступности в Российской Федерации, выявлены ключевые проблемы в данной сфере и обоснованы перспективные направления ее совершенствования.

Правовую основу противодействия компьютерной преступности в России составляет комплекс нормативных правовых актов различного уровня. Конституция Российской Федерации закрепляет основополагающие права граждан на неприкосновенность частной жизни, личную и семейную тайну, защиту своей чести и доброго имени, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений. Эти права непосредственно связаны с информационной сферой и требуют правовой защиты, в том числе уголовно-правовыми средствами.

Уголовный кодекс Российской Федерации содержит специальную главу 28 «Преступления в сфере компьютерной информации», включающую статьи 272 (неправомерный доступ к компьютерной информации), 273 (создание, использование и распространение вредоносных компьютерных программ), 274 (нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей), 274.1 (неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации). Помимо этого, уголовная ответственность за преступления, совершаемые с

использованием компьютерных технологий, предусмотрена в ряде других статей УК РФ, таких как статья 159.6 (мошенничество в сфере компьютерной информации), статья 171.2 (незаконные организация и проведение азартных игр), статья 242 (незаконные изготовление и оборот порнографических материалов или предметов) и другие.

Важными законодательными актами в сфере противодействия компьютерной преступности являются Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Федеральный закон от 28.12.2010 № 390-ФЗ «О безопасности». Существенное значение имеет также Доктрина информационной безопасности Российской Федерации, утвержденная Указом Президента РФ от 05.12.2016 № 646, определяющая стратегические цели и основные направления обеспечения информационной безопасности государства.

Несмотря на значительные изменения, внесенные в законодательство в последние годы, нормативно-правовая база противодействия компьютерной преступности не в полной мере соответствует современным вызовам в информационной сфере. Основной проблемой является отставание законодательства от темпов развития информационных технологий и новых форм киберпреступности. В частности, в уголовном законодательстве отсутствуют специальные составы для таких распространенных видов компьютерных преступлений, как фишинг (мошенничество, направленное на получение конфиденциальной информации), DDoS-атаки (распределенные атаки типа «отказ в обслуживании»), криптоджекинг (несанкционированное использование вычислительных ресурсов для добычи криптовалюты), кардинг (мошенничество с банковскими картами в сети Интернет). Эти деяния квалифицируются по общим статьям УК РФ, что затрудняет работу правоохранительных органов и не позволяет в полной мере учитывать специфику данных преступлений.

Еще одной проблемой является отсутствие в законодательстве четкого определения компьютерного преступления, что создает трудности в правоприменительной практике. В научной литературе и экспертном сообществе предлагаются различные подходы к определению данного понятия, однако единое понимание отсутствует. Законодательное закрепление понятия компьютерного преступления позволило бы устранить данную проблему и создать основу для дальнейшего совершенствования уголовного законодательства в данной сфере.

Значительные сложности возникают при расследовании компьютерных преступлений в связи с проблемами сбора и использования цифровых доказательств. Уголовно-процессуальное законодательство не содержит специальных норм, регулирующих порядок сбора, хранения и исследования электронных доказательств, что создает риски признания их недопустимыми. Необходимо совершенствование процессуального законодательства в части регламентации работы с цифровыми доказательствами, определения порядка проведения следственных действий в цифровой среде, использования специальных технических средств при расследовании компьютерных преступлений.

Существенной проблемой является отсутствие единообразной судебной практики по делам о компьютерных преступлениях. Анализ судебных решений показывает различные подходы к квалификации одних и тех же деяний, определению размера ущерба, назначению наказания. Для решения данной проблемы необходимо принятие руководящих разъяснений Верховного Суда РФ по вопросам применения законодательства о компьютерных преступлениях, обобщение и анализ судебной практики по данной категории дел.

В организационном аспекте противодействие компьютерной преступности в России обеспечивается деятельностью специализированных подразделений правоохранительных органов. Ключевую роль играет Управление «К» МВД России и его территориальные подразделения,

осуществляющие выявление, предупреждение, пресечение и раскрытие преступлений в сфере информационных технологий. В их компетенцию входит борьба с преступлениями в сфере компьютерной информации, противодействие мошенничеству в сети Интернет, пресечение распространения вредоносного программного обеспечения, выявление и пресечение фактов нарушения авторских и смежных прав в сети Интернет, противодействие распространению материалов порнографического характера с участием несовершеннолетних.

В структуре Федеральной службы безопасности Российской Федерации действуют Центр информационной безопасности и специализированные подразделения по борьбе с киберпреступностью. Они осуществляют деятельность по обеспечению информационной безопасности государства, противодействию иностранным техническим разведкам, защите сведений, составляющих государственную тайну, противодействию кибертерроризму и кибершпионажу.

Важной структурой в системе противодействия компьютерной преступности является Национальный координационный центр по компьютерным инцидентам (НКЦКИ), созданный в соответствии с Федеральным законом «О безопасности критической информационной инфраструктуры Российской Федерации». НКЦКИ осуществляет координацию деятельности субъектов критической информационной инфраструктуры по вопросам обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.

В рамках Следственного комитета Российской Федерации действуют специализированные подразделения по расследованию преступлений в сфере высоких технологий. Важную роль в системе противодействия компьютерной преступности играют также органы прокуратуры, осуществляющие надзор за исполнением законодательства в сфере информационной безопасности и противодействия киберпреступности.

Анализ деятельности указанных структур позволяет выявить ряд проблем, снижающих эффективность противодействия компьютерной преступности. Прежде всего, это недостаточное кадровое обеспечение специализированных подразделений. Несмотря на повышение престижа службы в данных структурах, сохраняется дефицит высококвалифицированных специалистов, обладающих необходимыми знаниями и навыками в области информационных технологий и методики расследования компьютерных преступлений. Особенно остро данная проблема стоит в региональных подразделениях правоохранительных органов.

Для решения кадровой проблемы необходимо создание специализированных образовательных программ, направленных на подготовку экспертов в области информационной безопасности для правоохранительных органов. Такие программы должны сочетать глубокие теоретические знания в области права и информационных технологий с практическими навыками выявления и расследования компьютерных преступлений. Целесообразно также развитие системы повышения квалификации сотрудников правоохранительных органов, занимающихся противодействием компьютерной преступности, включая организацию стажировок в ведущих российских и зарубежных центрах по борьбе с киберпреступностью. Важным направлением является повышение материального и социального обеспечения сотрудников специализированных подразделений, что позволит привлечь в их ряды высококвалифицированных специалистов из коммерческого сектора.

Вторая проблема связана с недостаточным материально-техническим обеспечением подразделений по борьбе с компьютерной преступностью. Расследование данного вида преступлений требует использования современного оборудования и специализированного программного обеспечения для анализа цифровых доказательств, восстановления удаленной информации, мониторинга сетевого трафика, исследования вредоносного

программного обеспечения. Однако во многих региональных подразделениях наблюдается недостаток такого оборудования, что существенно затрудняет работу по выявлению и расследованию компьютерных преступлений.

Для решения данной проблемы необходимо увеличение финансирования материально-технического обеспечения специализированных подразделений, закупка современных программно-аппаратных комплексов для проведения компьютерно-технических экспертиз. Особое внимание следует уделить разработке отечественного программного обеспечения для криминалистического анализа цифровых данных, что особенно важно в условиях санкционных ограничений и необходимости обеспечения технологической независимости в сфере информационной безопасности.

Третьей проблемой является отсутствие единой методики расследования компьютерных преступлений, учитывающей их специфику. Компьютерные преступления характеризуются особенностями механизма их совершения, спецификой следообразования, сложностью сбора и анализа цифровых доказательств. Отсутствие научно обоснованной методики расследования данного вида преступлений затрудняет работу следственных органов, приводит к ошибкам в квалификации деяний, утрате доказательственной информации.

Разработка и внедрение единой методики расследования компьютерных преступлений позволит повысить эффективность работы следственных органов, обеспечить единообразие практики расследования данного вида преступлений. Методика должна включать рекомендации по первоначальным и последующим следственным действиям, тактике проведения отдельных следственных действий при расследовании компьютерных преступлений, алгоритмы сбора и анализа цифровых доказательств, обеспечивающие их допустимость в уголовном процессе. Особое внимание следует уделить рекомендациям по взаимодействию следователей со специалистами в области

информационных технологий, назначению и проведению компьютерно-технических экспертиз.

Существенной проблемой в организации противодействия компьютерной преступности является недостаточная координация деятельности различных ведомств. Несмотря на создание координационных структур, таких как НКЦКИ, на практике наблюдаются сложности в обмене информацией между правоохранительными органами, отсутствие единых баз данных о киберинцидентах, дублирование функций различных подразделений. Это снижает оперативность реагирования на компьютерные преступления, затрудняет выявление и пресечение деятельности организованных преступных групп в сфере информационных технологий.

Для решения данной проблемы необходимо создание единой межведомственной системы противодействия компьютерной преступности, обеспечивающей оперативный обмен информацией и координацию действий всех заинтересованных структур. Такая система должна включать единую базу данных о киберинцидентах, механизмы оперативного взаимодействия между различными ведомствами, протоколы совместных действий при выявлении и расследовании компьютерных преступлений. Важным элементом системы должны стать ситуационные центры, обеспечивающие мониторинг информационного пространства, анализ киберугроз и координацию действий при реагировании на масштабные киберинциденты.

Технические меры противодействия компьютерной преступности включают в себя широкий спектр программно-технических средств и методов, направленных на защиту информационных систем и данных от несанкционированного доступа, модификации, уничтожения, а также на выявление и пресечение компьютерных атак. К таким мерам относятся внедрение систем обнаружения и предотвращения вторжений, средств криптографической защиты информации, механизмов аутентификации и авторизации пользователей, систем мониторинга и аудита информационной безопасности, средств резервного копирования и восстановления данных.

Особое значение имеет развитие отечественных технологий информационной безопасности, обеспечивающих защиту критической информационной инфраструктуры от внешних угроз. В условиях санкционных ограничений и рисков, связанных с использованием импортного программного обеспечения, создание отечественных средств защиты информации является стратегической задачей. В России реализуется политика импортозамещения в сфере информационных технологий, формируется реестр отечественного программного обеспечения, однако темпы развития отечественных технологий информационной безопасности недостаточны для обеспечения технологической независимости в данной сфере.

Одним из перспективных направлений развития технических мер противодействия компьютерной преступности является использование технологий искусственного интеллекта для выявления и предотвращения компьютерных атак. Системы, основанные на машинном обучении, способны анализировать большие объемы данных о сетевом трафике, выявлять аномалии и потенциальные угрозы, что позволяет оперативно реагировать на киберинциденты. Такие системы могут обнаруживать новые, ранее неизвестные виды атак, адаптироваться к изменяющимся тактикам киберпреступников, что особенно важно в условиях постоянно эволюционирующих угроз.

В России ведутся разработки систем защиты информации на основе искусственного интеллекта, однако их внедрение в практику противодействия компьютерной преступности происходит недостаточно активно. Необходимо стимулирование исследований и разработок в данной области, создание условий для внедрения перспективных технологий в государственных и коммерческих структурах, подготовка специалистов, способных разрабатывать и эксплуатировать такие системы.

Важным элементом технических мер противодействия компьютерной преступности является развитие методов компьютерно-технической экспертизы. Данная экспертиза играет ключевую роль в расследовании

компьютерных преступлений, обеспечивая сбор и анализ цифровых доказательств. В России действует ряд экспертных учреждений, осуществляющих компьютерно-технические экспертизы, однако их возможности не всегда соответствуют современным требованиям. Необходимо дальнейшее развитие экспертных учреждений, оснащение их современным оборудованием и программным обеспечением, подготовка высококвалифицированных экспертов в области информационных технологий.

Особое место в системе противодействия компьютерной преступности занимает государственно-частное партнерство. Большая часть информационной инфраструктуры находится в частной собственности, поэтому эффективное противодействие киберугрозам невозможно без активного участия бизнес-сообщества. Частные компании обладают значительными ресурсами и экспертизой в области информационной безопасности, что может быть использовано для повышения эффективности противодействия компьютерной преступности.

В России формируются механизмы взаимодействия государственных структур и частного сектора в сфере информационной безопасности, однако они требуют дальнейшего развития. Перспективным направлением является создание отраслевых центров обмена информацией о киберугрозах, объединяющих представителей государственных органов и коммерческих организаций. Такие центры могут обеспечивать обмен данными об инцидентах информационной безопасности, анализ новых видов киберугроз, разработку рекомендаций по защите информационных систем, проведение совместных учений по отражению кибератак.

Важным элементом государственно-частного партнерства является привлечение частных компаний к разработке технологий информационной безопасности, используемых в государственном секторе. Это может осуществляться через механизмы государственного заказа, создание совместных исследовательских центров, реализацию программ поддержки

отечественных разработчиков средств защиты информации. Такое взаимодействие позволит объединить ресурсы государства и бизнеса для решения стратегических задач в области информационной безопасности.

Учитывая транснациональный характер компьютерной преступности, важнейшим элементом системы противодействия является международное сотрудничество. Компьютерные преступления часто совершаются с территории одного государства против объектов, расположенных в другом государстве, что создает сложности в выявлении и преследовании преступников. Эффективное противодействие таким преступлениям возможно только при тесном взаимодействии правоохранительных органов разных стран.

Россия участвует в ряде международных инициатив в сфере противодействия компьютерной преступности, в том числе в рамках СНГ, ШОС, БРИКС. Важным шагом стало принятие резолюции Генеральной Ассамблеи ООН «Противодействие использованию информационно-коммуникационных технологий в преступных целях», инициированной Россией. Данная резолюция предусматривает разработку всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, что может стать основой для формирования глобальной системы противодействия киберпреступности.

Несмотря на эти усилия, полноценное международное сотрудничество в сфере противодействия компьютерной преступности затруднено политическими факторами. Россия не является участником Конвенции Совета Европы о киберпреступности (Будапештской конвенции), что ограничивает возможности взаимодействия с европейскими странами в данной сфере. Тем не менее, российские правоохранительные органы осуществляют сотрудничество с зарубежными коллегами в рамках двусторонних соглашений и международных организаций, таких как Интерпол.

Дальнейшее развитие международного сотрудничества требует совершенствования правовой базы, создания эффективных механизмов обмена информацией между правоохранительными органами разных стран, проведения совместных операций по выявлению и пресечению трансграничных компьютерных преступлений. Важным направлением является также гармонизация национальных законодательств в сфере противодействия компьютерной преступности, что облегчит международное сотрудничество и повысит эффективность борьбы с киберпреступностью на глобальном уровне.

Важнейшим направлением противодействия компьютерной преступности является профилактика. Значительная часть киберпреступлений становится возможной из-за низкого уровня осведомленности пользователей о правилах безопасного поведения в цифровой среде, несоблюдения базовых мер информационной безопасности, использования уязвимого программного обеспечения. В связи с этим, повышение уровня цифровой грамотности населения и формирование культуры информационной безопасности являются ключевыми элементами профилактики компьютерной преступности.

В России реализуются программы повышения цифровой грамотности населения, включая проект «Цифровая экономика Российской Федерации», предусматривающий развитие образовательных программ по информационной безопасности, проведение информационных кампаний, направленных на повышение осведомленности граждан о киберугрозах. Однако масштаб этих программ недостаточен для формирования общей культуры информационной безопасности в обществе.

Необходимо внедрение образовательных программ по основам информационной безопасности на всех уровнях образования, начиная с начальной школы и заканчивая высшими учебными заведениями. Такие программы должны включать как теоретические знания о принципах обеспечения информационной безопасности, так и практические навыки

защиты личной информации, безопасного использования интернет-сервисов, выявления признаков мошенничества в цифровой среде.

Важным элементом профилактики компьютерной преступности является проведение широких информационных кампаний, направленных на повышение осведомленности граждан о киберугрозах. Такие кампании должны включать социальную рекламу, публикации в СМИ, проведение тематических мероприятий, распространение информационных материалов о правилах безопасного поведения в цифровой среде. Особое внимание следует уделить защите наиболее уязвимых категорий пользователей, таких как дети, подростки и пожилые люди.

Профилактика компьютерной преступности в организациях включает внедрение политик информационной безопасности, проведение регулярных аудитов безопасности, обучение сотрудников правилам безопасной работы с информационными системами, реализацию технических мер защиты информации. В России действуют нормативные документы, определяющие требования к обеспечению информационной безопасности в государственных и коммерческих организациях, однако их соблюдение не всегда обеспечивается на должном уровне. Необходимо усиление контроля за выполнением требований информационной безопасности, особенно в организациях, обрабатывающих персональные данные граждан и другую чувствительную информацию.

Особое внимание следует уделить подготовке специалистов в области информационной безопасности. В России действует система высшего и дополнительного профессионального образования по данному направлению, однако существует разрыв между академической подготовкой и реальными потребностями рынка труда. Многие выпускники не обладают достаточными практическими навыками для эффективной работы в сфере информационной безопасности. Необходимо дальнейшее развитие образовательных программ, их адаптация к современным вызовам в сфере информационной безопасности,

увеличение количества практико-ориентированных курсов, развитие системы стажировок в профильных организациях.

Важным направлением подготовки специалистов является проведение соревнований по кибербезопасности, таких как CTF (Capture The Flag), киберучений, хакатонов. Такие мероприятия позволяют выявлять талантливых специалистов, развивать их навыки, формировать сообщество профессионалов в области информационной безопасности. В России проводится ряд подобных соревнований, включая международные, однако их масштаб и регулярность недостаточны для формирования полноценной системы подготовки кадров.

Анализ существующей системы противодействия компьютерной преступности в России позволяет сформулировать основные направления ее совершенствования. В правовой сфере необходимо дальнейшее развитие законодательства, направленное на криминализацию новых форм киберпреступности, уточнение существующих составов преступлений, совершенствование процессуальных норм, регламентирующих сбор и использование цифровых доказательств. Целесообразно закрепление в законодательстве понятия компьютерного преступления, разработка и принятие руководящих разъяснений Верховного Суда РФ по вопросам применения законодательства о компьютерных преступлениях.

В организационной сфере требуется укрепление специализированных подразделений правоохранительных органов, совершенствование их кадрового и материально-технического обеспечения, развитие механизмов межведомственной координации. Необходимо создание единой межведомственной системы противодействия компьютерной преступности, включающей единую базу данных о киберинцидентах, механизмы оперативного взаимодействия между различными ведомствами, ситуационные центры для мониторинга и координации действий при масштабных киберинцидентах.

В технической сфере необходимо стимулирование разработки и внедрения отечественных технологий информационной безопасности, развитие систем мониторинга и реагирования на киберинциденты, использование передовых технологий, включая искусственный интеллект, для выявления и предотвращения компьютерных атак. Важным направлением является развитие методов компьютерно-технической экспертизы, оснащение экспертных учреждений современным оборудованием и программным обеспечением, подготовка высококвалифицированных экспертов.

В сфере международного сотрудничества необходимо развитие правовой базы взаимодействия с зарубежными странами, активизация участия России в международных инициативах по противодействию киберпреступности, создание эффективных механизмов обмена информацией и проведения совместных операций с правоохранительными органами других стран.

В образовательной сфере требуется внедрение программ по информационной безопасности на всех уровнях образования, проведение широких информационных кампаний, направленных на повышение осведомленности граждан о киберугрозах, развитие системы подготовки специалистов в области информационной безопасности, включая проведение практико-ориентированных мероприятий, таких как соревнования по кибербезопасности.

Таким образом, противодействие компьютерной преступности представляет собой комплексную задачу, требующую согласованных усилий государственных органов, бизнес-сообщества, научных и образовательных организаций, гражданского общества. Только системный подход, учитывающий правовые, организационные, технические и образовательные аспекты, позволит создать эффективную систему противодействия данному виду преступности, соответствующую современным вызовам и угрозам в информационной сфере. Реализация предложенных мер будет способствовать снижению уровня компьютерной преступности, защите прав и законных

интересов граждан, организаций и государства в цифровой среде, обеспечению информационной безопасности Российской Федерации.

Подводя итоги третьей главы о проведении анализа организации и системы противодействия компьютерной преступности в России, мы пришли к следующим выводам.

Правовая основа включает комплекс нормативных актов, однако выявлен ряд проблем: отставание законодательства от развития технологий, недостаточная регламентация процедур сбора цифровых доказательств, а также проблемы в работе специализированных подразделений правоохранительных органов.

Технические меры противодействия включают внедрение систем защиты информации и развитие отечественных технологий безопасности. Особое значение приобретают технологии искусственного интеллекта для выявления кибератак, государственно-частное партнерство и международное сотрудничество в борьбе с киберпреступностью.

На основе анализа определены ключевые направления совершенствования системы: развитие законодательства, укрепление правоохранительных подразделений, стимулирование разработки отечественных технологий безопасности, расширение международного сотрудничества и внедрение образовательных программ по информационной безопасности. Эффективное противодействие компьютерной преступности требует системного подхода и согласованных действий всех заинтересованных сторон.

# Заключение

В рамках настоящего исследования нами был проведен комплексный анализ уголовной ответственности за преступления в сфере компьютерной информации, что позволило сформировать целостное представление о данном институте уголовного права и выявить существующие проблемы правового регулирования и правоприменительной практики.

Анализ исторического развития законодательства о преступлениях в сфере компьютерной информации показал, что его формирование происходило поэтапно, отражая эволюцию информационных технологий и осознание обществом опасности их противоправного использования. Первоначально компьютерные преступления не выделялись в отдельную категорию и квалифицировались по общим составам преступлений, таким как кража, мошенничество, нарушение тайны переписки.

По мере развития информационных технологий и увеличения их роли в экономической и социальной жизни общества происходило формирование специального законодательства о преступлениях в сфере компьютерной информации. В Российской Федерации данный процесс завершился включением в Уголовный кодекс 1996 года специальной главы 28 «Преступления в сфере компьютерной информации». В дальнейшем законодательство продолжало совершенствоваться, отражая появление новых форм компьютерной преступности и возрастающую общественную опасность данных деяний.

Исследование понятия и сущности компьютерной преступности позволило выявить ее основные характеристики, включая высокую латентность, транснациональный характер, значительный материальный и нематериальный ущерб, сложность выявления и расследования. Компьютерная преступность представляет собой динамичное явление, постоянно эволюционирующее вместе с развитием информационных технологий. Это создает значительные трудности для законодателя и

правоприменителя, вынужденных реагировать на новые формы противоправного поведения в цифровой среде. В научной литературе и правоприменительной практике отсутствует единообразное понимание компьютерной преступности, что затрудняет выработку эффективных мер противодействия данному явлению.

В рамках исследования предложено авторское определение компьютерного преступления как общественно опасного деяния, совершаемого с использованием компьютерных технологий либо направленного на компьютерную информацию и системы ее обработки, посягающего на информационную безопасность личности, общества и государства.

Анализ особенностей преступлений в сфере компьютерной информации показал, что они обладают спецификой, связанной с особым предметом посягательства – компьютерной информацией, использованием специальных технических средств и методов, а также наличием специфических следов преступления. Компьютерные преступления характеризуются особым механизмом следообразования, при котором следы преступления представляют собой изменения в компьютерной информации, что требует применения специальных методов их выявления и фиксации.

Преступления в сфере компьютерной информации могут совершаться дистанционно, что затрудняет установление личности преступника и привлечение его к ответственности. Значительная часть компьютерных преступлений имеет трансграничный характер, что создает сложности в определении юрисдикции и применимого права.

Исследование выявило недостаточность существующего понятийного аппарата для описания всего многообразия преступлений, совершаемых с использованием информационных технологий.

Действующее законодательство ограничивается понятием преступлений в сфере компьютерной информации, не охватывая все виды противоправных деяний, связанных с использованием информационных технологий.

Необходимо дальнейшее развитие понятийного аппарата в данной сфере для более эффективного правового регулирования и правоприменения.

Комплексный анализ объективных признаков компьютерных преступлений демонстрирует ярко выраженную специфику данной категории деяний, обусловленную особой природой цифрового пространства.

Родовым объектом рассматриваемых преступлений выступают общественные отношения в сфере обеспечения компьютерной безопасности.

Видовым объектом выступают отношения, обеспечивающие безопасность компьютерной информации и правомерное использование компьютерных систем.

Непосредственными объектами конкретных составов преступлений являются более узкие группы общественных отношений, таких как безопасность компьютерной информации, правомерный доступ к компьютерной информации, целостность и доступность компьютерной информации, безопасность информационно-телекоммуникационных сетей и так далее.

Предметом преступного посягательства служит компьютерная информация, обладающая уникальными свойствами: нематериальностью,

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

Субъективные признаки компьютерных преступлений характеризуются преимущественно умышленной формой вины (прямой или косвенный умысел), за исключением нарушения правил эксплуатации средств хранения информации, где допустима и неосторожная форма вины. Мотивационная сфера этих преступлений отличается многообразием (корыстные,

хулиганские, политические мотивы), что в ряде случаев выступает квалифицирующим признаком.

Субъектом в большинстве составов является физическое вменяемое лицо, достигшее 16-летнего возраста, хотя для некоторых составов преступлений законодатель устанавливает специальный субъект.

Квалифицирующие признаки преступлений в сфере компьютерной информации обнаруживают определенную системность. Типичными квалифицирующими обстоятельствами выступают совершение деяния группой лиц по предварительному сговору или организованной группой.

Проведенный анализ в исследовании также выявил проблемы квалификации новых форм киберпреступлений (фишинг, кибersталкинг, DDoS-атаки), которые часто не имеют прямого отражения в уголовном законодательстве и квалифицируются по общим составам преступлений. Это указывает на необходимость совершенствования уголовного законодательства в данной сфере.

В ходе исследования был проведен анализ организации и системы мер противодействия компьютерной преступности и выявлены основные проблемы в данной сфере, обоснованы перспективные направления ее совершенствования.

Исследование показало, что эффективное противодействие компьютерной преступности возможно только при системном подходе, включающем правовые, организационные, технические и образовательные меры. Правовая основа противодействия компьютерной преступности в России представлена комплексом нормативных актов, включающих Конституцию РФ, Уголовный кодекс РФ, федеральные законы «Об информации, информационных технологиях и о защите информации», «О безопасности критической информационной инфраструктуры Российской Федерации», Доктрину информационной безопасности Российской Федерации. Несмотря на значительные изменения, внесенные в законодательство в последние годы, нормативно-правовая база не в полной

мере соответствует современным вызовам в информационной сфере. Основными проблемами являются отставание законодательства от темпов развития информационных технологий, отсутствие специальных составов для новых видов компьютерных преступлений, недостаточная регламентация процедуры сбора и использования цифровых доказательств. В организационном аспекте противодействие компьютерной преступности обеспечивается деятельностью специализированных подразделений правоохранительных органов, включая Управление «К» МВД России, подразделения ФСБ России, Национальный координационный центр по компьютерным инцидентам. Анализ их деятельности выявил ряд проблем, включая недостаточное кадровое и материально-техническое обеспечение, отсутствие единой методики расследования компьютерных преступлений, недостаточную координацию деятельности различных ведомств. Технические меры противодействия компьютерной преступности включают внедрение систем обнаружения и предотвращения вторжений, средств криптографической защиты информации, механизмов аутентификации и авторизации пользователей, систем мониторинга и аудита информационной безопасности. Особое значение имеет развитие отечественных технологий информационной безопасности, обеспечивающих защиту критической информационной инфраструктуры от внешних угроз. Перспективным направлением является использование технологий искусственного интеллекта для выявления и предотвращения компьютерных атак, развитие методов компьютерно-технической экспертизы. Важным элементом системы противодействия компьютерной преступности является государственно-частное партнерство. Большая часть информационной инфраструктуры находится в частной собственности, поэтому эффективное противодействие киберугрозам невозможно без активного участия бизнес-сообщества. Перспективным направлением является создание отраслевых центров обмена информацией о киберугрозах, привлечение частных компаний к разработке технологий информационной безопасности для государственного сектора.

Учитывая транснациональный характер компьютерной преступности, особое значение приобретает международное сотрудничество. Россия участвует в ряде международных инициатив в данной сфере, однако полноценное взаимодействие затруднено политическими факторами.

Необходимо дальнейшее развитие правовой базы международного сотрудничества, создание эффективных механизмов обмена информацией и проведения совместных операций с правоохранительными органами других стран, гармонизация национальных законодательств.

Профилактика компьютерной преступности является важнейшим направлением противодействия данному явлению. Значительная часть киберпреступлений становится возможной из-за низкого уровня осведомленности пользователей о правилах безопасного поведения в цифровой среде. Необходимо внедрение образовательных программ по основам информационной безопасности на всех уровнях образования, проведение широких информационных кампаний, направленных на повышение осведомленности граждан о киберугрозах.

Особое внимание следует уделить подготовке специалистов в области информационной безопасности, развитию практико-ориентированных образовательных программ, проведению соревнований по кибербезопасности. На основе проведенного анализа сформулированы основные направления совершенствования системы противодействия компьютерной преступности.

В правовой сфере необходимо дальнейшее развитие законодательства, направленное на криминализацию новых форм киберпреступности, уточнение существующих составов преступлений, совершенствование процессуальных норм.

В организационной сфере требуется укрепление специализированных подразделений правоохранительных органов, создание единой межведомственной системы противодействия компьютерной преступности.

В технической сфере необходимо стимулирование разработки и внедрения отечественных технологий информационной безопасности, развитие систем мониторинга и реагирования на киберинциденты.

В сфере международного сотрудничества необходимо развитие правовой базы взаимодействия с зарубежными странами, активизация участия России в международных инициативах.

В образовательной сфере требуется внедрение программ по информационной безопасности, проведение информационных кампаний, развитие системы подготовки специалистов.

Таким образом, компьютерная преступность является динамично развивающимся явлением, формы и методы совершения компьютерных преступлений постоянно совершенствуются, что требует своевременного реагирования со стороны законодателя и правоприменительных органов. В связи с этим представляется необходимым проведение дальнейших научных исследований в данной области с учетом современных тенденций развития информационных технологий и их влияния на формирование новых видов общественно опасных деяний. Особое внимание следует уделить исследованию проблем уголовной ответственности за преступления, связанные с использованием искусственного интеллекта, технологий виртуальной и дополненной реальности, облачных вычислений и иных перспективных направлений развития информационных технологий.

## Список используемой литературы и используемых источников


1. Арямов А.А. Компьютерные преступления: юридическая характеристика, алгоритмы квалификации, практика правоприменения : монография / А.А. Арямов, Ю.В. Грачева, А.И. Чучаев. – Москва : Проспект, 2020. 240 с.

2. Бегишев И.Р. Понятие и особенности преступлений против компьютерной информации / И.Р. Бегишев // Вестник Казанского юридического института МВД России. 2013. № 12. С. 126-130.

3. Букалерова Л.А. Специфика уголовно-правовой охраны информационной безопасности / Л.А. Букалерова, А.В. Остроушко // Общество и право. 2014. № 2. С. 91-97.

4. Ветров Н.И. Уголовное право. Особенная часть: учебник для вузов / Н.И. Ветров. – Москва : ЮНИТИ-ДАНА, 2016. 543 с.

5. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – Москва : Юрлитинформ, 2002. 496 с.

6. Гаврилин Ю.В. Расследование неправомерного доступа к компьютерной информации: учебное пособие / Ю.В. Гаврилин. – Москва : Книжный мир, 2001. 88 с.

7. Гаджиев М.С. Криминологический анализ преступности в сфере компьютерной информации: по материалам Республики Дагестан : Автореф. дис. канд. юр. наук. – Махачкала, 2018. 210 с.

8. Дворецкий М.Ю. Преступления в сфере компьютерной информации (уголовно-правовое исследование) : монография / М.Ю. Дворецкий. – Тамбов : Издательство ТГУ им. Г.Р. Державина, 2019. 182 с.

9. Евдокимов К.Н. Противодействие компьютерным преступлениям: теория, законодательство, практика : монография / К.Н. Евдокимов. – Иркутск : Иркутский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2020. 390 с.

10. Евдокимов К.Н. Уголовно-правовые и криминологические аспекты противодействия преступлениям в сфере компьютерной информации: монография / К.Н. Евдокимов. – Иркутск : ИрГУ, 2018. 267 с.

11. Жмыхов А.А. Компьютерная преступность за рубежом и ее предупреждение / А.А. Жмыхов // Известия Тульского государственного университета. 2014. № 2. С. 184-190.

12. Зинина У.В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: Автореф. дис. канд. юр. наук. - Москва, 2018. 180 с.

13. Зубова М.А. Компьютерная информация как объект уголовно-правовой охраны : Автореф. дис. канд. юр. наук. – Казань, 2019. 211 с.

14. Комментарий к Уголовному кодексу Российской Федерации (постатейный) / под редакцией А.И. Рарога. – 12-е изд., перераб. и доп. – Москва : Проспект, 2022. 912 с.

15. Комментарий к Уголовному кодексу Российской Федерации / Под ред. В.М. Лебедева. – Москва : Юрайт, 2020. 1032 с.

16. Крылов, В.В. Информационные компьютерные преступления / В.В. Крылов. – Москва: ИНФРА-М-НОРМА, 1997. 285 с.

17. Крылов В.В. Информационные компьютерные преступления / В.В. Крылов. – Москва : ИНФРА-М-НОРМА, 2018. 285 с.

18. Лопатина Т.М. Криминологические и уголовно-правовые основы противодействия компьютерной преступности: монография / Т.М. Лопатина. – Москва: Юрлитинформ, 2006. 192 с.

19. Лопатина Т.М. Теоретические и методологические основы уголовно-правовой охраны компьютерной информации : монография / Т.М. Лопатина. – Москва : Юрлитинформ, 2020. 440 с.

20. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия: учебно-практическое пособие / В.А. Мазуров. – Москва : Палеотип, 2002. 148 с.

21. Мазуров, В.А. Преступления в сфере информационных технологий: классификация, квалификация, расследование : монография / В.А. Мазуров. – Барнаул : Издательство Алтайского университета, 2018. 168 с.

22. Постановление Пленума Верховного Суда РФ от 30.11.2017 № 48 «О судебной практике по делам о мошенничестве, присвоении и растрате» (ред. от 15.12.2022) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_283918/ (дата обращения 10.03.2024)

23. Рарог, А.И. Субъективная сторона и квалификация преступлений : монография / А.И. Рарог. - Москва : Проспект, 2021. 232 с.

24. Рарог, А.И. Уголовное право России. Части Общая и Особенная: учебник / А.И. Рарог. – Москва : Проспект, 2020. 896 с.

25. Репецкая А.Л. Киберпреступность: уголовно-правовой и криминологический аспекты / А.Л. Репецкая, Б.А. Тугутов // Всероссийский криминологический журнал. 2019. Т. 13, № 3. С. 416-425.

26. Рогозин В.Ю. Преступления в сфере компьютерной информации: уголовно-правовая характеристика и проблемы квалификации / В.Ю. Рогозин. – Москва : ЮНИТИ-ДАНА, 2018. 159 с.

27. Русскевич Е.А. Дифференциация ответственности за преступления, совершаемые с использованием информационно-коммуникационных технологий, и проблемы их квалификации: монография / Е.А. Русскевич. – Москва: Юрлитинформ, 2018. 232 с.

28. Русскевич Е.А. Уголовно-правовое противодействие преступлениям, совершаемым с использованием информационно-коммуникационных технологий : монография / Е.А. Русскевич. – Москва : ИНФРА-М, 2019. 188 с.

29. Степанов-Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации : монография / В.Г. Степанов-Егиянц. – Москва : Статут, 2019. 175 с.

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

31. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы: монография / Т.Л. Тропина. Владивосток: Изд-во Дальневост. ун-та, 2009. 240 с.

32. Тропина Т.Л. Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы : монография / Т.Л. Тропина. - Владивосток : Издательство Дальневосточного университета, 2021. 240 с.

33. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 28.02.2025) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_10699/ (дата обращения 10.03.2024).

34. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ (последняя редакция) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 10.03.2024).

35. Федеральный закон «О внесении изменений в отдельные законодательные акты Российской Федерации и приостановлении действия отдельных положений законодательных актов Российской Федерации» от 19.12.2022 № 519-ФЗ (последняя редакция) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_434564/ (дата обращения 10.03.2024).

36. Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ (последняя редакция) [Электронный ресурс] URL: https://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения 10.03.2024).

37. Хисамова З.И. Уголовно-правовые меры противодействия преступлениям, совершаемым в финансовой сфере с использованием информационно-телекоммуникационных технологий : специальность 12.00.08 «Уголовное право и криминология; уголовно-исполнительное право» : диссертация на соискание ученой степени кандидата юридических наук / Хисамова Зарина Илдузовна ; Краснодарский университет МВД России. – Краснодар, 2018. 222 с. Библиогр.: с. 195-221. Текст : непосредственный.

38. Шагиева Р.В. Преступления в сфере компьютерной информации: проблемы теории, законодательной регламентации и правоприменения / Р.В. Шагиева, В.А. Казакова // Ученые труды Российской академии адвокатуры и нотариата. 2016. № 2. С. 59-64.

39. Щетинина А.С. Конфиденциальная компьютерная информация как объект уголовно-правовой охраны / А.С. Щетинина // Вестник Омского университета. Серия «Право». 2015. № 2. С. 221-226.

40. Яни П.С. Субъективные признаки преступлений в сфере экономической деятельности: проблемы доказывания / П.С. Яни. – Текст : непосредственный // Российская юстиция. 2019. № 9. С. 23-27. ISSN 0131-6761.