

ГЛОБАЛЬНАЯ ПОЛИТИКА В СФЕРЕ УГОЛОВНО-ПРАВОВОЙ ЗАЩИТЫ ОБЩЕСТВА ОТ КИБЕРПРЕСТУПНОСТИ: МЕЖДУНАРОДНЫЕ ОБЯЗАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ ПРИ РАТИФИКАЦИИ КОНВЕНЦИИ ООН (2024)

Денис Валентинович Пучков

Уральский государственный юридический университет им. В. Ф. Яковлева,
г. Екатеринбург, Российская Федерация
d.puchkov@loys.law

 <https://orcid.org/0000-0002-5318-0338>

Аннотация. Настоящая статья посвящена анализу эволюции глобальной уголовно-правовой политики в контексте противодействия киберпреступности. Особое внимание уделяется процессу принятия Конвенции Организации Объединенных Наций по использованию информационно-коммуникационных технологий в преступных целях (далее — Конвенция ООН против киберпреступности), принятой 24 декабря 2024 года Генеральной Ассамблеей ООН (Резолюция 79/243), ее имманентной правовой природе и потенциальным импликациям для государств-участников. Проводится анализ возможных обязательств Российской Федерации в случае ратификации данного международного инструмента, охватывающий аспекты адаптации уголовного и уголовно-процессуального законодательства, интенсификации трансграничного сотрудничества, а также преодоления институциональных вызовов. В заключение постулируется императивная необходимость применения системного подхода к процессу имплементации положений Конвенции в национальную правовую систему.

Ключевые слова: киберпреступность, международное сотрудничество, уголовная политика, Конвенция ООН 2024, Российская Федерация, электронные доказательства

Для цитирования: Пучков Д. В. Глобальная политика в сфере уголовно-правовой защиты общества от киберпреступности: международные обязательства Российской Федерации при ратификации Конвенции ООН (2024) // Правопорядок: история, теория, практика. 2025. № 3(46). С. 147–153. DOI: 10.47475/2311-696X-2025-46-3-147-153

Research article

GLOBAL POLICY IN THE FIELD OF CRIMINAL LAW PROTECTION OF SOCIETY FROM CYBERCRIME: INTERNATIONAL OBLIGATIONS OF THE RUSSIAN FEDERATION UPON RATIFICATION OF THE UN CONVENTION (2024)

Denis V. Puchkov

Ural State Law University name after V. F. Yakovlev, Yekaterinburg, Russian Federation
d.puchkov@loys.law

 <https://orcid.org/0000-0002-5318-0338>

Abstract. This article analyzes the evolution of global criminal law policy in the context of combating cybercrime. Special attention is paid to the process of adopting the United Nations Convention on the Use of Information and Communications Technologies for Criminal Purposes (hereinafter — Convention against cybercrime), adopted on December 24, 2024, by the UN General Assembly (Resolution 79/243), its inherent legal nature, and potential implications for participating states. A meticulous analysis is conducted regarding the possible obligations of the Russian Federation upon ratification of this international instrument, covering aspects of adapting criminal and criminal procedural legislation, intensifying cross-border cooperation, and overcoming institutional challenges. The conclusion postulates the imperative necessity of applying a systemic approach to the process of implementing the Convention's provisions into the national legal system.

Keywords: cybercrime, international cooperation, criminal policy, UN Convention 2024, Russian Federation, electronic evidence

For citation: Puchkov DV. Global Policy in the Field of Criminal Law Protection of Society from Cybercrime: International Obligations of the Russian Federation upon Ratification of the UN Convention (2024). *Pravoporyadok: istoriya, teoriya, praktika* [Legal and Order: History, Theory, Practice]. 2025;(3):147-153. (In Russ.) DOI: 10.47475/2311-696X-2025-46-3-147-153

Введение

Экспоненциальный рост информационных технологий и стремительная цифровизация всех аспектов жизнедеятельности, от макроэкономических систем до механизмов государственного управления, привели к беспрецедентному масштабированию феномена киберпреступности. Данное явление, детерминируемое трансграничной природой и динамичным развитием новых схем преступления, представляет собой серьезную экзистенциальную угрозу для национальной безопасности суверенных государств, стабильности глобальных финансовых систем и фундаментальных прав индивидуумов в мировом масштабе. В ответ на эти появляющиеся вызовы международное сообщество инициировало проактивные шаги по выработке унифицированных подходов к уголовно-правовой экспликации и защите от киберпреступных деяний. Кульминацией этих многосторонних усилий явилось принятие 24 декабря 2024 года Конвенции № 79/243 Организации Объединенных Наций против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям (далее — Конвенция ООН против киберпреступности)¹, призванной сформировать универсальный нормативно-правовой базис для эффективного противодействия данному виду делинквентности.

Настоящее исследование посвящено критическому анализу этой новой международной инициативы и ее потенциальных импликаций для правовой системы Российской Федерации. Актуальность данного изыскания детерминируется императивом комплексной оценки готовности российского законодательства к имплементации положений Конвенции и адаптации к формирующимся международным стандартам в сфере борьбы с киберпреступностью.

Материалы и методы

Методологическая основа данного исследования базируется на компаративном анализе международных

правовых актов, нормативно-правовой базы Российской Федерации, а также доктринальных источников в области международного уголовного права, киберправа и криминологии. В работе использованы как общенаучные методы, включая системный анализ, синтез, индукцию, дедукцию и типологизацию, так и частнонаучные подходы, в частности, сравнительно-правовой и формально-юридический анализ. Особый акцент сделан на компаративном сопоставлении положений Конвенции ООН против киберпреступности с действующим законодательством Российской Федерации и релевантными международными актами, такими как Европейская конвенция Совета Европы по киберпреступлениям (далее — Будапештская конвенция)², с целью идентификации потенциальных коллизий и перспектив гармонизации правовых норм. Эмпирическая база включает официальные документы ООН, законодательные акты и экспертные заключения ведущих научно-исследовательских институтов.

Описание исследования

Принятая 24 декабря 2024 года Генеральной Ассамблеей ООН Конвенция против киберпреступности репрезентирует собой эпохальное событие в эволюции международного публичного права. Данный документ конституирует универсальный многосторонний международный договор, разработанный под эгидой Организации Объединенных Наций, что говорит об его глобальном характере и потенциале для широкой ратификации государствами-членами. В отличие от региональных инструментов, таких как Будапештская конвенция Совета Европы, Конвенция ООН стремится к охвату максимально возможного числа государств, предлагая унифицированный стандарт противодействия киберпреступности. Ее правовая природа определяется как обязывающее многостороннее соглашение, влекущее за собой для государств-участников обязательства по криминализации определенных видов деяний, интенсификации международного сотрудничества и имплементации процессуальных механизмов, необходимых для эффективной борьбы с киберпреступностью. Принципиальным аспектом является ее потенциал стать основополагающим элементом для дальнейшего прогрессивного развития международного уголовного права в сфере высоких технологий, обеспечивая универсальный правовой механизм про-

¹ Конвенция ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно — Коммуникационных систем, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям № 79/243, Принята Резолюцией Генеральной Ассамблеи ООН от 24 декабря 2024 года // URL: <https://docs.un.org/ru/A/RES/79/243> (дата обращения: 15.06.2025).

² Европейская конвенция по киберпреступлениям (преступлениям в киберпространстве): заключена в Будапеште 23 ноября 2001 г. // СПС «Гарант». URL: <https://base.garant.ru/4089723/> (дата обращения: 15.06.2025).

тивоедействия преступлениям, имманентно лишенным национальных юрисдикционных границ.

Процесс принятия Конвенции ООН по ИКТ завершился консенсусным одобрением ее финальной версии всеми 193 государствами — членами Организации Объединенных Наций. Данное значимое событие было формализовано путем принятия Резолюции 79/243 Генеральной Ассамблеи ООН без проведения голосования 24 декабря 2024 года, что подчеркивает высокий уровень межгосударственного согласия по ключевым аспектам регулирования киберпреступности. Согласно установленным процедурам международного права, Конвенция будет открыта для подписания на торжественной церемонии в Ханое в октябре 2025 года. После этого возможность подписания сохранится в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке до 31 декабря 2026 года. Вступление Конвенции в силу обусловлено депонированием сорокового документа о ратификации, принятии, утверждении или присоединении, что соответствует стандартной практике универсальных международных договоров и обеспечивает ее широкое правовое действие.

Принятие Конвенции ООН против киберпреступности знаменует собой фундаментальный этап в консолидации глобальных усилий по противодействию транснациональной киберпреступности. Данный международный инструмент направлен на унификацию базовых уголовно-правовых и процессуальных подходов, что является критически важным для обеспечения эффективности борьбы с преступлениями, по своей природе не имеющими национальных границ. Унификация осуществляется по нескольким ключевым направлениям, охватывая материальные составы преступлений, механизмы взаимной правовой помощи, экстрадицию, а также специфические процедуры, касающиеся электронных доказательств.

Конвенция предписывает государствам-участникам криминализовать определенные деяния, связанные с ИКТ, устанавливая минимальные стандарты для элементов их составов. Это позволяет гармонизировать национальные уголовные законодательства и минимизировать риск существования «лакун» или различий, препятствующих международному сотрудничеству.

Однако категориальный аппарат Конвенции ООН против киберпреступности не содержит дефиниции «компьютерная информация», что, на наш взгляд, выглядит абсолютно логично, с учетом того, что международные конвенции стремятся к технологической нейтральности, что означает их независимость от конкретных аппаратных и программных решений или форматов данных. Использование обобщенного термина «информация» позволяет избежать устаревания правовых норм вследствие стремительного научно-технического прогресса и смены доминирующих технологий. Это придает конвенциям долгосрочную релевантность и адаптивность. В рамках международно-правовых парадигм понятие «информация» трактуется максимально широко, охватывая совокупность любых

данных, независимо от их формы представления, способа создания или носителя. Компьютерная информация в данном контексте является лишь одной из модальностей более объемного концепта. Такой подход обеспечивает инклюзивность и применимость нормативных актов ко всем видам данных, циркулирующих в ИКТ-среде.

Определение «компьютерной информации» может существенно различаться в национальных законодательствах и доктринальных подходах различных государств. Универсализация данного термина на международном уровне сопряжена с риском возникновения коллизий и интерпретационных разногласий.

Таким образом, отсутствие прямого упоминания «компьютерной информации» в Конвенции ООН по ИКТ является результатом осознанного выбора в пользу концептуальной широты, технологической нейтральности, минимизации дефиниционных споров и приоритизации вопросов безопасности в международно-правовом регулировании сферы ИКТ.

При этом в конвенции представлено понятие «электронные данные», что на наш взгляд является прогрессивным и более перспективным подходом с учетом развития технологий. Так, согласно п. б) статьи 2 Конвенции ООН против киберпреступности «электронные данные» означают любое представление фактов, информации или концепций в форме, пригодной для обработки в информационно-коммуникационной системе, включая соответствующую программу, в результате действия которой информационно-коммуникационная система выполняет ту или иную функцию.

Нами ранее было представлено схожее по своей сути понятие компьютерной информации, где под компьютерной информацией предлагалось понимать любые сведения (сообщения, базы данных и т. д.), созданные либо преобразованные с помощью кибернетических технологий, находящихся либо имеющих следы в кибернетическом пространстве, либо зафиксированные в информационно-телекоммуникационной сети, системе или на машинном носителе [9, с. 241].

В свою очередь, понятие коммуникационной системы представлено в пункте а) статьи 2 Конвенции ООН против киберпреступности как любое устройство или группа соединенных или взаимосвязанных устройств, одно или несколько из которых по команде программы производит сбор, хранение и автоматическую обработку электронных данных.

Исходя из этого, компьютерная информация либо электронные данные, по своей сути, являются нематериальной сущностью. Они представляют собой совокупность сведений, сообщений или данных, лишенных физической формы. Их существование проявляется через абстрактные модели поведения и структуры, которые могут быть закодированы и интерпретированы. Несмотря на то, что компьютерная информация требует физического субстрата для своей фиксации (например, изменения магнитных полей на жестком диске, зарядов в полупроводниковых ячейках флеш-памяти или электрических сигналов в сети), эти материальные

носители являются лишь средством её репрезентации и хранения, а не самой информацией. Информация как таковая обладает информационным, а не вещественным атрибутом.

В свою очередь, информационно-коммуникационная система (ИКС), в отличие от информации и данных, обладает материальной и логически структурированной природой, включающей в себя: осязаемые устройства, такие как процессоры, память, сетевое оборудование, периферийные устройства, которые формируют материальную основу системы и наборы инструкций (алгоритмов), которые управляют аппаратными средствами, обеспечивают обработку данных, взаимодействие между компонентами и функционирование всей системы в целом. Эти компоненты, хотя и не имеют физической массы, являются неотъемлемой частью ИКС, определяя её поведение и функциональность.

В итоге ИКС выступает как функциональный комплекс, предназначенный для сбора, хранения, обработки и передачи электронных данных (компьютерной информации), обеспечивая её жизненный цикл в цифровой среде, и именно незаконный доступ к такого рода данным говорит о высокой общественной опасности.

Однако существующая уголовно-правовая охрана компьютерной информации в Российской Федерации существенно отличается от предложений в Конвенции по ИКТ.

Так, в части 1 статьи 7 Конвенции ООН по ИКТ предлагается криминализировать «Незаконный доступ к информационно-телекоммуникационной системе (Illegal Access)», а именно умышленный и неправомерный доступ ко всей информационно-коммуникационной системе или любой её части. Ключевым аспектом унификации здесь является требование квалификации данного деяния как формального состава преступления. Это означает, что для наступления уголовной ответственности не требуется обязательного причинения материального ущерба или иных последствий (уничтожения, модификации, блокирования информации), достаточным является сам факт неправомерного проникновения, особенно если оно сопряжено с преодолением мер защиты. Данный подход направлен на защиту конфиденциальности и неприкосновенности информационно-коммуникационных систем как таковых.

Однако согласно части 2 статьи 7 Конвенции ООН по ИКТ: «Государство-участник может установить требование, чтобы правонарушение было совершено путем нарушения мер безопасности с намерением получить электронные данные или с иным бесчестным или преступным умыслом, либо в отношении информационно-коммуникационной системы, соединенной с другой информационно-коммуникационной системой»¹. В дан-

ном случае предметом преступления выступают электронные данные.

Следует отметить, что построение уголовно-правовых норм стало развиваться на границе так называемых информационных преступлений и компьютерных преступлений. По мнению ряда исследователей, понятие «преступления, совершенного в информационном пространстве», должно раскрывать «любые противоправные деяния, осуществляемые благодаря компьютерной системе или сети, в этих системах или против компьютерных систем или сети» [12; 13].

Так, с учетом вышесказанных предложений, предлагается криминализировать незаконный доступ как к информационно — коммуникационной системе, так и к электронным данным (компьютерной информации), при этом состав преступлений в обоих предложениях является формальным по отношению к последствиям, в отличие от статьи 272 УК РФ, где требуется наступление последствий в виде уничтожения, модификации, блокирования либо копирования информации.

Необходимо указать на то, что на сегодняшний день предмет преступлений в сфере компьютерной информации намного шире и представляет собой информационно-телекоммуникационные сети и информацию, содержащуюся в критической информационной инфраструктуре Российской Федерации [9, с. 241].

Раскрытие содержания объективной стороны состава преступления, связанного с неправомерным доступом к компьютерной информации, осуществляется непосредственно в тексте ст. 272 УК РФ: «Неправомерный доступ к охраняемой законом информации», что определяет основные элементы объективной стороны рассматриваемого состава преступления.

С технической точки зрения неправомерный доступ понимается как «доступ к определенной информации, который был получен благодаря несанкционированному преодолению аппаратных, программных или комплексных мер защиты» [10, с. 32–35]. Иначе говоря, доступ всегда предполагает совершение совокупности тех действий, которые подпадают под определение: «активное поведение человека, заключающееся в воздействии на окружающую среду» [8, с. 56]. При этом некоторые исследователи считают, что в основе содержания неправомерности доступа лежит отсутствие добровольного согласия обладателя той или иной информации относительно возможностей доступа к ней:

- «без согласия собственника этой информации либо иного лица, обладающего ею по закону»²;
- «лицо не имеет права на доступ к компьютерной информации; лицо имеет право на доступ к данной информации, однако осуществляет его помимо установ-

нием № 79/243, Принята Резолюцией Генеральной Ассамблеи ООН от 24 декабря 2024 года // URL: <https://docs.un.org/ru/A/RES/79/243> (дата обращения: 15.06.2025).

² Уголовный кодекс Российской Федерации. Постатейный комментарий / науч. ред. Н. Ф. Кузнецова, Г. М. Миньковский. М.: ЗЕРЦАЛО: ТЕИС, 1997. С. 82.

ленного порядка, с нарушением правил эксплуатации» [5, с. 653];

– «несанкционированное владельцем информации ознакомление с данными, содержащимися на машинных носителях или компьютере, лица, не имеющего соответствующего допуска» [4, с. 664].

При этом следует учитывать и то, что в содержании ст. 272 УК РФ охрана информации не ставится в зависимость от уровня ее технической защищенности. Таким образом, неправомерным может быть признан и доступ к охраняемой законом информации при нахождении определенной информации на компьютере и без средств ее защиты определенными способами.

Среди основных способов осуществления неправомерного доступа выделяются использование чужого логина, изменение сетевого адреса технического устройства, завладение различными способами паролем, определение и использование существующих «пробелов» в программном обеспечении или сетевой защите, любой иной обман системы защиты компьютерной информации [7, с. 11]. При этом ущерб при неправомерном доступе к компьютерной информации может быть причинен в четырех основных формах (детальный юридический анализ которых был успешно выполнен в работе В. Г. Степанова-Егянца) [11] последствий:

- блокирование компьютерной информации, которое состоит в возможности или невозможности использования определенной компьютерной информации;
- копирование компьютерной информации;
- модификация компьютерной информации, т. е. осуществление преобразования, видоизменения компьютерной информации с приобретением ею новых свойств;
- уничтожение компьютерной информации.

По нашему мнению, последствия, указанные в ст. 272 УК РФ, в виде уничтожения, блокирования, модификации могут и должны образовывать составы самостоятельных преступлений, учитывая их посягательства на совершенно иные общественные отношения, нежели неправомерный доступ к компьютерной информации.

На наш взгляд, законодателем абсолютно необоснованно оставляются вне уголовно-правового запрета такие действия, как уничтожение, блокирование, модификация и копирование компьютерной информации. Между тем можно утверждать, что целью являются именно данные действия, а не сам по себе неправомерный доступ к компьютерной информации, который фактически стал вторичным по отношению к последствиям.

«Уголовная политика любого государства должна основываться на четком и ясном понимании того, каких изменений в состоянии, структуре и динамике преступности можно будет добиться, совершенствуя соответствующие институты и нормы», — говорили А. И. Алексеев, В. С. Овчинский и Ф. Э. Побегайло [1, с. 144].

Однако криминализация, на наш взгляд, и прежде всего вновь возникающих общественных отношений

в сфере телекоммуникаций, крайне необходима, но при наличии определенных факторов, а не в угоду сиюминутным потребностям государства.

Так, А. И. Коробеев указывал: «В результате объективного и закономерного процесса постоянного развития, изменения и совершенствования социальных структур, появления новых общественных отношений возникает необходимость в уголовно-правовой защите некоторых из них. Установлением уголовной наказуемости деяний, способных причинить вред вновь возникающим общественным отношениям, и обеспечивается такая защита. Отмеченная тенденция является отражением принципа динамизма в уголовном праве. Он, как известно, требует постоянного учета изменений в системе общественных отношений и своевременного отражения их в законе» [6, с. 247].

Тем не менее опираться на один лишь фактор динамизма недопустимо в силу необходимости наличия нескольких факторов, находящихся в системе и позволяющих ставить вопрос о криминализации того или иного общественно опасного деяния. Однако в вопросе сущности и количества данных факторов также нет единого мнения.

На наш взгляд, при конструировании нормы статьи Седьмой Конвенции ООН по ИКТ полностью выдержано правило построения диспозиций уголовно-правовой нормы, сформулированное М. И. Ковалевым: «чем абстрактнее описаны действия, образующие объективную сторону состава преступления, тем конкретнее должны быть указаны последствия этих действий. И наоборот» [3, с. 73].

Такого рода криминализация позволит выстроить более эффективную уголовно-правовую модель защиты телекоммуникаций от преступных посягательств, затрагивающих совершенно разные объекты уголовно-правовой охраны.

Некоторые страны криминализуют простой доступ, в то время как другие ограничивают криминализацию только преступлениями при действующей системе защиты и принимаемых мерах безопасности, или когда преступник имеет намерения незаконно получить данные, изменить их или нанести ущерб [2, с. 60]. В частности, Конвенция Совета Европы о киберпреступности включает положение о незаконном доступе, защищающем целостность компьютерных систем путем криминализации несанкционированного доступа к ней. Отмечая непоследовательность подходов на национальном уровне, Конвенция о киберпреступности предлагает возможность не применять государствами-участниками некоторые содержащиеся в ней положения при уже имеющихся в национальном законодательстве ограничениях, тем самым сохраняя собственные, в определенном смысле более либеральные законы о незаконном доступе к компьютерным системам. Данное положение направлено на защиту целостности всех компьютерных систем.

В этой связи представляется абсолютно логичным и обоснованным изменение ст. 272 УК РФ как в части

предмета преступления, так и в части наступления последствий, выделив существующие последствия в отдельные составы преступлений, изложив редакцию ст. 272 УК РФ в следующей редакции: «Неправомерный доступ к охраняемой законом компьютерной информации или информационно — телекоммуникационной системе либо его части».

Основанием для такой криминализации, помимо вышесказанных и научно обоснованных принципов криминализации, может стать ратификация Конвенции ООН по ИКТ, которая предполагает для Российской Федерации ряд существенных обязательств, требующих методологически выверенного и системного подхода к имплементации ее положений в национальную правовую систему. Данные обязательства охватывают как сферы материального уголовного права, так и регламентацию уголовно-процессуальной деятельности, а также способы международного сотрудничества и обеспечения прав человека.

Одним из ключевых императивов при ратификации Конвенции станет необходимость внесения комплексных корректив в Уголовный кодекс Российской Федерации. Это может быть связано с криминализацией новых видов деяний, ассоциированных с киберпреступностью, или с уточнением существующих составов преступлений с целью обеспечения их соответствия международно-правовым стандартам. Вероятно, потребуются ревизия ряда определений в сфере цифровой преступности для достижения унификации с конвенционными положениями, а также установление адекватных мер уголовной ответственности. Приоритетное внимание должно быть уделено составам, касающимся неправомерного доступа к компьютерной информации, разработки и распространения вредоносных компьютерных программ, мошенничества, совершаемого с использованием информационно-телекоммуникационных технологий, а также преступлений против целостности, конфиденциальности и доступности компьютерных данных и систем.

Однако реализация положений Конвенции, особенно в части экспансии полномочий правоохранительных органов по доступу к данным и осуществлению мониторинга, может генерировать определенные правозащитные вызовы. Императивно необходимо будет обеспечить оптимальный баланс между эффективностью противодействия киберпреступности и неукоснительным соблюдением конституционных прав граждан на неприкосновенность частной жизни, тайну переписки и защиту персональных данных. Это потребует создания строгих механизмов судебного контроля и прокурорского надзора за действиями субъектов правоприменения, а также обеспечения гарантий соразмерности и необходимого применения принудительных мер, как подчеркивается в аналитических отчетах правозащитных организаций.

В этой связи вспоминается бурная дискуссия в рамках Специального комитета ООН относительно принятия положений о соблюдении прав человека в со-

ответствии с Международным пактом о гражданских и политических правах человека (МПГПП), не ратифицированным рядом государств-участников¹. Результатом данных дискуссий стал итоговый компромисс, указанный в ст. 6 Конвенции против киберпреступности, который не в полной мере удовлетворил пожелания ряда сторон относительно строгих гарантий прав человека в контексте расследования киберпреступлений. Конвенция прежде всего сосредоточена на укреплении международного сотрудничества в борьбе с преступлениями, совершаемыми с использованием ИКТ, и в обмене доказательствами, а не на детальной регламентации прав человека, что делает ее более слабой в этой части по сравнению с Будапештской Конвенцией (2001).

Кроме того, несмотря на заявленный универсальный характер ряда положений Конвенции ООН против киберпреступности, Конвенция содержит ряд положений, которые потенциально могут быть предметом многосторонних дискуссий и иметь специфические национальные интерпретации. Российская Федерация на этапе формирования Конвенции могла артикулировать определенные оговорки или занимать особую позицию по некоторым принципиальным вопросам, касающимся, например, определения юрисдикции, объема международного сотрудничества или подходов к обеспечению кибербезопасности. Принципиально важно провести детальный анализ этих дискуссионных моментов и эксплицировать, каким образом позиция Российской Федерации по ним будет рефлексировать на процесс ратификации и последующую имплементацию. Это также включает вопросы, сопряженные с концепцией государственного суверенитета в киберпространстве и регуляторной политикой в отношении глобальной сети Интернет.

Заключение

Принятие Конвенции ООН против ИКТ представляет собой значимый этап в процессе формирования и консолидации глобальной уголовно-правовой политики в сфере противодействия киберпреступности. Для Российской Федерации ратификация данного международного договора сопряжена с императивом глубокой и системной реформы ряда сегментов национального законодательства, включая нормы уголовного и уголовно-процессуального права. Помимо адаптации нормативно-правовой базы, потребуются интенсификация механизмов международного сотрудничества и поиск оптимального баланса между эффективностью правоприменения и обеспечением защиты прав человека. Имплементация Конвенции будет требовать не только юридических, но и существенных институциональных, а также ресурсных импликаций, направленных на создание полноценной и когерентной системы противо-

¹ «Международный пакт о гражданских и политических правах человека» (Принят 16.12.1966 Резолюцией 2200 (XXI) на 1496-м пленарном заседании Генеральной Ассамблеи ООН) // СПС «КонсультантПлюс». URL: https://www.consultant.ru/document/cons_doc_LAW_5531/ (дата обращения: 15.06.2025).

действия киберпреступности в полном соответствии с международными стандартами, которые мы попытались раскрыть в данной статье на примере изменений ст. 272 УК РФ. Комплексный и научно обоснованный подход к решению этих задач позволит Российской Фе-

дерации эффективно участвовать в глобальной борьбе с киберпреступностью, обеспечивая безопасность своих граждан и критически важных информационных систем.

Список источников

1. Алексеев А. И., Овчинский В. С., Побегайло Ф. Э. Российская уголовная политика: преодоление кризиса. М.: Норма, 2006. 144 с.
2. Зинина У. В. Преступления в сфере компьютерной информации в российском и зарубежном уголовном праве: дис. ... канд. юрид. наук: 12.00.08. М., 2007. 160 с.
3. Ковалев М. И. Оптимальное соотношение формального и оценочного в уголовном законе // Советское государство и право. 1973. № 11. С. 68–74.
4. Комментарий к Уголовному кодексу Российской Федерации / отв. ред. А. В. Наумов. М.: Юристъ, 1996. 824 с.
5. Комментарий к Уголовному кодексу Российской Федерации / под общ. ред. д-ра юрид. наук, проф. Ю. И. Скуратова и В. М. Лебедева. М.: ИНФРА-М: Норма, 1996. 653 с.
6. Коробеев А. И. Уголовно-правовая политика России: от генезиса до кризиса. М.: Юрлитинформ. 247 с.
7. Ляпунов Ю. И., Максимов В. Ю. Ответственность за компьютерные преступления // Законность. 1997. № 1. С. 8–15.
8. Парфенов А. Ф. Общее учение об объективной стороне преступления: дис. ... канд. юрид. наук: 12.00.08. СПб., 2004. 428 с.
9. Пучков Д. В. Уголовно-правовая модель защиты телекоммуникаций от преступных посягательств: проблемы теории и практики: дис. ... д-ра юрид. наук: 5.1.4. Пучков Денис Валентинович. Екатеринбург, 2022. 474 с.
10. Сизов А. В. Неправомерный доступ к компьютерной информации: практика правоприменения // Информационное право. 2009. № 1. С. 32–35.
11. Степанов-Егиянц В. Г. Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект): дис. ... д-ра юрид. наук: 12.00.08 / Степанов-Егиянц Владимир Георгиевич. Москва, 2016. 389 с.
12. Lounsbury D. J. Information systems law and operator liability revisited // Murdoch university E-Law journal. 1994. Vol. 1. September, 3;
13. McMahon J. Practical decent security // Digital systems journal. 1992. Vol. 14. November.

СВЕДЕНИЯ ОБ АВТОРЕ

Пучков Денис Валентинович

Доктор юридических наук, профессор, Уральский государственный юридический университет имени В. Ф. Яковлева
Россия, 620066, г. Екатеринбург, ул. Комсомольская, д. 21
E-mail: d.puchkov@loys.law
ORCID: 0000-0002-5318-0338

INFORMATION ABOUT THE AUTHOR

Denis V. Puchkov

Doctor of Legal Sciences, Professor, Ural State Law University named after V. F. Yakovlev
21, Komsomolsk str., Yekaterinburg 620066, Russia
E-mail: d.puchkov@loys.law
ORCID: 0000-0002-5318-0338

КОНФЛИКТ ИНТЕРЕСОВ

Конфликт интересов отсутствует.

CONFLICT OF INTEREST

There is no conflict of interest.

Дата поступления статьи / Received: 25.06.2025.

Дата рецензирования статьи / Revised: 15.07.2025.

Дата принятия статьи к публикации / Accepted: 15.08.2025.