



Значение Конвенции ООН против киберпреступности для уголовного закона России

В. Н. Щепетильников

Кандидат юридических наук, доцент,
доцент кафедры юриспруденции им. В. Г. Ермакова

Елецкий государственный университет им. И. А. Бунина
399770, Россия, г. Елец, ул. Коммунаров, 28

E-mail: vic80@rambler.ru

Аннотация: в статье автор рассматривает недавно принятую Организацией Объединенных Наций и подписанную 74 государствами Конвенцию против киберпреступности в связке с Уголовным кодексом РФ и оценивает ее значение для последующего правоприменения в российской правовой системе. Очевидно, что многие из положений Конвенции уже нашли свое отражение в статьях Особенной части УК РФ с момента его принятия в 1996 году, а также в изменениях, принятых позднее. Несомненно, что ряд положений Конвенции станут в дальнейшем правовым ориентиром для правоприменительных и судебных органов власти. Несомненно и то, что роль Конвенции будет оценена по справедливости позднее, когда между странами, принявшими этот международный документ, наладится взаимодействие, во многом утраченное из-за политической конъюнктуры.

Ключевые слова: киберпреступление; уголовная ответственность; уголовное наказание; уголовный закон

© Щепетильников В. Н., 2026



Эта работа распространяется по лицензии CC BY 4.0.
Чтобы просмотреть копию этой лицензии, посетите
<https://creativecommons.org/licenses/by/4.0/>

The Significance of the UN Convention Against Cybercrime for the Criminal Law of Russia

V. N. Shchepetilnikov

Bunin Yelets State University
28, Kommunarov st., Yelets, 399770, Russia

E-mail: vic80@rambler.ru

Abstract: *in the article, the author discusses the Convention on Cybercrime, recently adopted by the United Nations and signed by 74 countries, in conjunction with the Criminal Code of the Russian Federation, and assesses its implications and significance for future law enforcement in the Russian legal system. It is evident that many of the provisions of the convention have already been incorporated into the articles of the Special Part of the Criminal Code of Russia since its adoption in 1996 and subsequent amendments. Undoubtedly, several provisions of the convention will serve as a legal guide for law enforcement and judicial authorities in the future. The significance of these provisions will be more clearly understood later, when cooperation among the countries that have adopted this international instrument is established, a process that has been hindered by political circumstances.*

Keywords: *cybercrime; criminal liability; criminal punishment; criminal law*

25 октября 2025 года в Ханое (Вьетнам) произошло мировое событие, которое Президент РФ назвал «без преувеличения историческим»: была подписана Конвенция Организации Объединенных Наций против киберпреступности¹ (далее – Конвенция). Россия еще в 2019 году выступила с инициативой по разработке такого универсального международного договора о противодействии использованию информационно-коммуникационных технологий в преступных целях. «Преступления такого рода, зачастую тесно связанные с терроризмом и пропагандой экстремистской идеологии, незаконным оборотом наркотиков и оружия, представляют серьезную угрозу безопасности как отдельных граждан, так и целых государств. ...Россия открыта к самому тесному международному сотрудничеству в сфере борьбы с киберпреступностью», – говорится на сайте Кремля².

Отечественные средства массовой информации и прочие информационные ресурсы обошли это событие стороной. И только специалисты, имеющие отношение

¹ Конвенция 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: принята резолюцией 79/243 Ген. Ассамблеи ООН от 24 дек. 2024 г.

² Участникам и гостям церемонии подписания Конвенции ООН против киберпреступности: [приветствие В. В. Путина]. URL: <http://kremlin.ru/events/president/letters/78291>.

к данному документу, могут себе представить значение его для международного права и нашей правовой системы.

В сообщении Министерства иностранных дел Российской Федерации³ отмечалось, что это первый юридически обязывающий договор в области международной информационной безопасности, нацеленный «на укрепление международного правоохранительного сотрудничества по противодействию использованию информационно-коммуникационных технологий в преступных целях». Государства-члены ООН призывались к подписанию Конвенции, обеспечению условий для ее скорейшего вступления в силу, наращиванию политико-дипломатических усилий «по выполнению согласованных взаимных обязательств и совершенствованию конвенционных механизмов сотрудничества». Россия со своей стороны подтвердила «приверженность задаче всеобъемлющего противодействия использованию информационно-коммуникационных технологий в преступных целях, обозначенной в резолюции Генеральной Ассамблеи ООН 74/247»⁴.

На V Международной научно-практической конференции «Проблемы обеспечения верховенства закона: история и современность» (Хвостовские чтения) в г. Липецке глава АНО «Белый Интернет» доктор юридических наук, профессор Э. Л. Сидоренко, выступая на пленарном заседании, рассказала, каких усилий стоило делегации РФ приблизить день подписания Конвенции, какие трудности и препоны создавались представителями недружественных иностранных государств, чтобы осложнить принятие данного документа⁵.

Российскую Федерацию в Ханое представлял генеральный прокурор А. В. Гуцан, который возглавлял официальную делегацию и был уполномочен подписать Конвенцию⁶ и огласить послание Президента РФ В. В. Путина участникам церемонии подписания. Накануне Правительством РФ в соответствии со статьей 9 Федерального закона «О международных договорах Российской Федерации»⁷ было принято постановление с одобрением представленного МИД РФ, согласованного с Минюстом РФ, МВД РФ, Минцифры РФ, ФСБ РФ, СВР РФ, Генпрокуратурой РФ и СК РФ предложения о подписании Россией Конвенции ООН.

В международном правовом поле до настоящего времени существовал только один конвенционный документ, направленный на сотрудничество между государствами и частным сектором в борьбе против преступности в сфере компьютерной

³ О подписании Конвенции ООН против киберпреступности: [сообщение для СМИ]. URL: https://www.mid.ru/ru/foreign_policy/un/2055536/.

⁴ Противодействие использованию информационно-коммуникационных технологий в преступных целях. Резолюция Ген. Ассамблеи ООН от 27 дек. 2019 г. URL: <https://docs.un.org/ru/A/RES/74/247>.

⁵ URL: <https://t.me/cryptoelina/7017>.

⁶ О подписании Конвенции 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: Распоряжение Президента Рос. Федерации от 23 окт. 2025 г. № 409-рп.

⁷ О международных договорах Российской Федерации: Федер. закон от 15 июля 1995 г. № 101-ФЗ: принят Гос. Думой 16 июня 1995 г. (ред. 08.12.2020).

информации и утверждающий необходимость защиты законных интересов в сфере использования и развития информационных технологий, – Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001 г.), вступившая в силу 1 июля 2004 года. Однако Российская Федерация в этом договоре не участвовала – якобы из-за того, что считает его «инструментом вмешательства во внутренние дела других государств и нарушения их суверенитета»⁸. На самом деле разногласия здесь лежат в практической плоскости: документ 2001 года не может учитывать все изменившиеся отношения и виды киберпреступлений⁹.

Международное сообщество в целом и Россию в частности всегда волновало использование информационно-коммуникационных систем при совершении уголовных правонарушений, включая правонарушения, связанные с терроризмом и транс-национальной организованной преступностью, такие как торговля людьми, незаконный ввоз мигрантов, незаконное изготовление и оборот огнестрельного оружия, его составных частей, компонентов и боеприпасов к нему, незаконный оборот наркотиков и незаконный оборот культурных ценностей. Еще на XI Конгрессе ООН по предупреждению преступности и уголовному правосудию, проходившем в Бангкоке в 2005 году, было отмечено, что для эффективности взаимной правовой помощи определения основных преступлений и процессуальные полномочия, существующие в одной стране, должны соответствовать аналогичным положениям, действующим в другой стране¹⁰. Вот и преамбула нынешней Конвенции против киберпреступности исходит в числе прочего из необходимости «принятия соответствующего законодательства, установления общих составов преступлений и процессуальных полномочий и укрепления международного сотрудничества в целях более эффективного предупреждения такой деятельности и противодействия ей на национальном, региональном и международном уровнях».

Во-первых, Конвенция содержит ряд терминов, в частности «информационно-коммуникационная система», «электронные данные», «данные о трафике», которые ранее в национальном законодательстве России не раскрывались, если не считать определения информационной системы и информационно-телекоммуникационной сети, электронного сообщения и трафика, закрепленные в двух федеральных законах – «Об информации, информационных технологиях и о защите информации»¹¹ и «О связи»¹². В то же время в Конвенции по-прежнему отсутствуют понятия киберпре-

⁸ Скобликов П. А. Анализ проекта всеобъемлющей конвенции ООН против киберпреступности в контексте соблюдения прав пострадавших // Актуальные проблемы российского права. 2025. Т. 20, № 11. С. 101.

⁹ См. об этом подробнее: Кузнецов А. Г. Международное сотрудничество в борьбе с киберпреступностью // Научный портал МВД России. 2023. № 1 (61). С. 131–136.

¹⁰ 11-й Конгресс ООН по предупреждению преступности и уголовному правосудию. Документы. URL: <https://www.un.org/ru/events/11thcongress/documents.html>.

¹¹ Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 г. № 149-ФЗ: принят Гос. Думой 8 июля 2006 г.: одобрен Советом Федерации 14 июля 2006 г. (ред. от 29.12.2025).

¹² О связи: Федер. закон от 7 июля 2003 г. № 126-ФЗ: принят Гос. Думой 18 июня 2003 г.: одобрен Советом Федерации 25 июня 2003 г. (ред. от 20.02.2026).

ступности и киберпреступления; предлагается лишь некое «основное преступление», под которым понимается любое преступление, принесшее доходы, в отношении которых могут быть совершены преступления, указанные в статье 17 настоящей Конвенции, а также «серьезное преступление», наказуемое лишением свободы на максимальный срок не менее четырех лет или предусматривающее более строгую меру наказания. Применительно к классификации преступлений по Уголовному кодексу РФ¹³ (далее – УК РФ) это преступления средней тяжести и более тяжкие деяния. В связи с отсутствием определения термина «киберпреступность» немало состоялось споров и было внесено предложений, и все же предпочтительной остается точка зрения, согласно которой в таком определении нет необходимости, ибо «совершение новых видов киберпреступлений может не подпадать под ответственность, и это приведет к нарушению принципа неотвратимости наказания»¹⁴.

В остальном для единообразного правопонимания и оперирования одинаковыми категориями в нашем внутреннем законодательстве должны быть выработаны (или приведены в соответствие с текстом Конвенции) аналогичные термины и определения. Так, например, в УК РФ в настоящее время используется термин «информационно-телекоммуникационные сети», характеризующий объективную сторону отдельных преступных деяний с учетом их специфики. В примечании к статье 187 УК РФ о неправомерном обороте средств платежей применено словосочетание «с использованием информационно-коммуникационных технологий», что хотя и созвучно понятийному аппарату Конвенции, однако отличается от него. Это важно, поскольку статья 4 Конвенции четко говорит о необходимости признания «конвенционных» преступлений уголовными и по внутреннему законодательству, «если они совершаются с использованием информационно-коммуникационных систем». В то же время в примечаниях к статье 2 Конвенции указано, что «государства-участники не обязаны дословно воспроизводить в своем внутреннем законодательстве те же термины, определения которых даны в статье 2 Конвенции, при условии, что их законодательство охватывает эти понятия таким образом, что это соответствует принципам и целям Конвенции и обеспечивает эквивалентные рамки для ее осуществления».

Во-вторых, в главе II Конвенции о криминализации называются и описываются конкретные составы преступлений, которые должны быть включены во внутреннее законодательство страны-участницы. Как следует из научной статьи А. А. Бессонова о киберпреступлениях, «в России наибольший рост... характерен для преступлений в сфере компьютерной информации (почти в 13 раз), далее следуют незаконный оборот наркотиков (в 3,3 раза), мошенничество (в 3 раза), преступления экстремистской и террористической направленности (в 2 раза), распространение порнографических

¹³ Уголовный кодекс Российской Федерации: Федер. закон от 13 июня 1996 г. № 63-ФЗ: принят Гос. Думой 24 мая 1996 г.: одобрен Советом Федерации 5 июня 1996 г. (ред. от 20.02.2026).

¹⁴ Булгаков С. С., Поздняков А. Н. О новых терминах в сфере отечественной правоохранительной деятельности: «киберпреступность» // Труды Академии управления МВД России. 2022. № 4 (64). С. 81.

материалов (в 1,5 раза). Между тем отмечается снижение количества краж и случаев организации азартных игр»¹⁵.

Если же проводить параллели между УК РФ и Конвенцией ООН, чтобы оценить готовность России к международному взаимодействию в рамках данного международного документа, мы приходим к следующим выводам.

Положения статьи 7 Конвенции о незаконном доступе и статьи 9 о воздействии на электронные данные уже давно включены в состав статьи 272 УК РФ.

Статья 8 Конвенции о незаконном перехвате отражается отчасти в статьях 138.1, 272.1 и 283.1 УК РФ.

Статья 10 Конвенции о воздействии на информационно-коммуникационную систему находит свое выражение в статьях 274 и 274.1 УК РФ.

Статья 11 Конвенции, криминализирующая «получение, производство, продажу, приобретение для использования, ввоз, распространение или предоставление иным способом... устройств, включая программное обеспечение, разработанных или адаптированных прежде всего для целей совершения какого-либо из преступлений, признанных таковыми в соответствии со статьями 7–10 настоящей Конвенции», – это нынешние статьи 272.1, 273, 274.3–274.5 УК РФ.

Статья 12 Конвенции о подлоге с применением информационно-коммуникационной системы – это статьи 285.3, 292, 322.1, 327 и некоторые другие в УК РФ.

Статья 13 Конвенции о хищении или мошенничестве с использованием информационно-коммуникационной системы сегодня представлена в статье 159.6 УК РФ.

Статья 14 Конвенции о преступлениях, связанных с размещением в Интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации, включена по смыслу в статьи 242.1 и 242.2 УК РФ. В исследовании Л. Л. Бошаевой, посвященном криминологическим характеристикам киберпреступности в отношении несовершеннолетних, справедливо отмечается, что «в настоящее время все большее число растлителей малолетних используют компьютерные технологии для создания и пополнения личных порнографических коллекций с образами детей, что также способствует совершению развратных действий и иных сексуальных преступлений в отношении несовершеннолетних»¹⁶.

Статья 15 Конвенции о домогательстве или создании доверительных отношений с целью совершения сексуального преступления в отношении ребенка отчасти находит свое выражение в статье 133 УК РФ, однако нашему законодательству, и уголовному закону в частности, незнакомо такое выражение, как «домогательство».

Статья 16 Конвенции о криминализации распространения интимных изображений без согласия соответствует статье 137 УК РФ. Вместе с тем, по нашему мнению, в целях дальнейшей разработки положений статьи 16 Конвенции представляется возможным включение (уточнение) в УК РФ составов преступлений, связанных с продажей, распространением, передачей, публикацией или предоставлением иным

¹⁵ Бессонов А. А. Киберпреступность: тенденции и перспективы // Расследование преступлений: проблемы и пути их решения. 2024. № 3 (45). С. 25.

¹⁶ Бошаева Л. Л. Криминологическая характеристика киберпреступности в отношении несовершеннолетних в России: моногр. М.: Проспект, 2023. С. 38.

способом интимного изображения человека с помощью информационно-коммуникационной системы без согласия лица, представленного на этом изображении, с конкретизацией мотивов и целей совершаемых деяний, в том числе в отношении несовершеннолетних от 14 до 18 лет. Причем в указанной статье Конвенции дается определение «интимного изображения» для целей единообразного применения.

Статья 17 Конвенции об отмыывании доходов от преступлений давно нашла свое подтверждение в статьях 174 и 174.1 УК РФ.

Новеллой для нашего уголовного законодательства, хотя и давно уже последовательно отстаиваемой, в частности, Следственным комитетом РФ, является положение статьи 18 Конвенции об ответственности юридических лиц. Правда, в части 2 статьи сделана оговорка, что «в зависимости от правовых принципов государства-участника ответственность юридических лиц может быть уголовной, гражданско-правовой или административной». Причем уточняется, что «такая ответственность действует без ущерба для уголовной ответственности физических лиц, совершивших преступления».

Характерно, что Конвенция не называет конкретного срока давности привлечения к ответственности по вышеназванным преступлениям, обозначая его как «длительный» и «более продолжительный» и тем самым предоставляя это право государствам-участникам.

Любопытно, что в числе отягчающих Конвенция называет обстоятельства, «затрагивающие критическую информационную инфраструктуру» (ст. 21). Как известно, в УК РФ данное обстоятельство вынесено в отдельный состав статьи 274.1 УК РФ без отнесения его к отягчающим.

В-третьих, глава III Конвенции затрагивает вопросы юрисдикции государств-участников в отношении совершаемых преступлений, что созвучно положениям статей 11–13 УК РФ в части действия правил (принципов) гражданства, территории.

Многие положения главы IV Конвенции посвящены процессуальным и правоприменительным мерам, однако это тема для отдельного анализа и разговора. Следует лишь подчеркнуть, что многие из них касаются актуальных вопросов сохранения и обеспечения электронных доказательств.

Заслуживает серьезного внимания статья 31 Конвенции о замораживании, аресте и конфискации доходов от преступлений, поскольку обозначенные в ней правовые инструменты выступают не в качестве мер уголовного наказания, а скорее как меры процессуального обеспечения производства по делу о киберпреступлении. Кроме того, безотносительно к тексту Конвенции крайне любопытным представляется опыт Китайской Народной Республики в использовании для борьбы с киберпреступностью «нового вида альтернативного наказания, называемого “массовые неудобства”, за которое следует на определенный срок социальная изоляция в стране – блокируются мобильные платежи, виновное лицо может использовать только наличные деньги»¹⁷.

¹⁷ Наумов Ю. Г., Самолысов П. В., Тришкина Е. А. Правовые и экономические инструменты противодействия киберпреступности в Российской Федерации // Труды Академии управления МВД России. 2024. № 3 (71). С. 63.

Значительная часть положений в главе V Конвенции касается процедур международного сотрудничества в обозначенной сфере, включая защиту персональных данных, выдачу преступников, оказание взаимной правовой помощи¹⁸. Особое значение в настоящее время приобретает сотрудничество между правоохранительными органами, однако существующие политические разногласия нередко его осложняют и этим наносят ущерб общим интересам сохранения законности и правопорядка в странах мира. В этом смысле Конвенция является действительно основой для взаимного сотрудничества между правоохранительными органами в отношении киберпреступлений, наносящих серьезный вред уголовно охраняемым интересам любой страны. Безусловно позитивным шагом является признание возможности проведения заинтересованными компетентными органами совместных расследований (ст. 48 Конвенции).

Немаловажным остается и предупреждение совершения киберпреступлений на территории стран-участниц (глава VI Конвенции), что, по мнению авторов документа, возможно посредством принятия надлежащих законодательных, административных или других мер (ст. 53). Причем немалая роль отводится здесь неправительственным организациям, организациям гражданского общества, научным учреждениям и структурам частного сектора, общественности в целом. Собственно, в такой связке под эгидой государства в России и работают общественные институты.

Существенным, на наш взгляд, является положение пункта 4 статьи 53 Конвенции, обязывающее страны-участницы принимать надлежащие меры к тому, чтобы «соответствующий компетентный орган или органы, ответственные за предупреждение киберпреступности и борьбу с ней, были известны и доступны населению для направления им в надлежащих случаях сообщений, в том числе анонимных, о любых инцидентах, которые могут быть квалифицированы как уголовные правонарушения, признанные таковыми в соответствии с настоящей Конвенцией». Это особенно важно с позиций статьи 141 УПК РФ и статьи 11 Федерального закона от 2 мая 2006 г. № 59-ФЗ «О порядке рассмотрения обращений граждан Российской Федерации».

Остается добавить, что Конвенцию подписали 74 государства (!), что, несомненно, стало дипломатической победой нашей страны. Этот процесс и является примером транснациональной криминализации¹⁹. В соответствии со статьей 64 Конвенция будет открыта для подписания всеми государствами и региональными организациями экономической интеграции в штаб-квартире Организации Объединенных Наций в Нью-Йорке до 31 декабря 2026 года. Конвенция вступит в силу на девятый день после даты сдачи на хранение сорокового документа о ратификации, принятии, утверждении или присоединении (по состоянию на 7 февраля 2026 года еще не вступила в силу).

¹⁸ См.: Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // Вестник Санкт-Петербургского университета. Право. 2022. Т. 13, вып. 3. С. 678–695.

¹⁹ Карпика А. Г., Захаров Н. Д. Актуальные вопросы транснациональной криминализации киберпреступности // Философия права. 2025. № 1 (112). С. 109–114.

Таким образом, Конвенция является ориентиром для нашего законодателя в дальнейшем совершенствовании уголовного закона. Ее положения во многом уже включены в содержание статей Особенной части УК РФ. Вместе с тем ряд положений Кодекса, а также специального законодательства нуждаются в уточнении или дополнении.

Библиографический список

Бессонов А. А. Киберпреступность: тенденции и перспективы // *Расследование преступлений: проблемы и пути их решения.* 2024. № 3 (45). С. 23–30. DOI: 10.54217/2411-1627.2024.45.3.002.

Бошаева Л. Л. Криминологическая характеристика киберпреступности в отношении несовершеннолетних в России: моногр. М.: Проспект, 2023.

Булгаков С. С., Поздняков А. Н. О новых терминах в сфере отечественной правоохранительной деятельности: «киберпреступность» // *Труды Академии управления МВД России.* 2022. № 4 (64). С. 76–82. DOI: 10.24412/2072-9391-2022-464-76-82.

Карпика А. Г., Захаров Н. Д. Актуальные вопросы транснациональной криминализации киберпреступности // *Философия права.* 2025. № 1 (112). С. 109–114.

Клевцов К. К. Международное сотрудничество в борьбе с киберпреступностью в контексте противодействия новым вызовам и угрозам // *Вестник Санкт-Петербургского университета. Право.* 2022. Т. 13, вып. 3. С. 678–695. DOI: 10.21638/srbu14.2022.306.

Кузнецов А. Г. Международное сотрудничество в борьбе с киберпреступностью // *Научный портал МВД России.* 2023. № 1 (61). С. 131–136.

Наумов Ю. Г., Самолысов П. В., Тришкина Е. А. Правовые и экономические инструменты противодействия киберпреступности в Российской Федерации // *Труды Академии управления МВД России.* 2024. № 3 (71). С. 58–65. DOI: 10.24412/2072-9391-2024-371-58-65.

Скобликов П. А. Анализ проекта всеобъемлющей конвенции ООН против киберпреступности в контексте соблюдения прав пострадавших // *Актуальные проблемы российского права.* 2025. Т. 20, № 11. С. 99–112. DOI: 10.17803/1994-1471.2025.180.11.099-112.

Цифровое право: учеб. / [Я. О. Алимова, Л. В. Андреева, В. С. Белых и др.]; под общ. ред. проф. В. В. Блажеева, проф. М. А. Егоровой. 2-е изд., перераб. и доп. М.: Проспект, 2025.

Информация для цитирования

Щепетильников В. Н. Значение конвенции ООН против киберпреступности для уголовного закона России // *Ex jure.* 2026. № 2. С. 135–143. DOI: 10.17072/2619-0648-2026-2-135-143. EDN DQSXMG

Shchepetilnikov V. N. The Significance of the UN Convention Against Cyber-crime for the Criminal Law of Russia. *Ex jure.* 2026. № 2. Pp. 135–143. DOI: 10.17072/2619-0648-2026-2-135-143. EDN DQSXMG
