https://doi.org/10.38044/2686-9136-2025-6-11

СТАТЬИ

КОНВЕНЦИЯ ООН ПРОТИВ КИБЕРПРЕСТУПНОСТИ: ИСТОРИЯ И ПРАВОВЫЕ ПЕРСПЕКТИВЫ

Л. В. Божко[1,2]

[1]Московский государственный институт международных отношений (университет) МИД России
119454, Россия, Москва, пр. Вернадского, 76

[2]Райффайзенбанк
119002, Россия, Москва, пл. Смоленская-Сенная, 28

Аннотация

В результате стремительного развития информационных технологий и роста киберпреступности обеспечение международной информационной безопасности становится важнейшей задачей мирового сообщества. Статья анализирует перспективы принятой 24 декабря 2024 г. Конвенции ООН против киберпреступности как механизма координации усилий государств в области обеспечения международной информационной безопасности. Цель исследования заключается в оценке данного международного договора в качестве основы для сотрудничества государств в сфере международной информационной безопасности и противодействия киберпреступности. Особое внимание уделяется положениям Конвенции, касающимся обязанности государства криминализировать устанавливаемый договором перечень деяний, а также проблеме соблюдения прав человека в связи с ее применением. В ходе исследования автором были использованы историко-правовой, формально-юридический и сравнительно-правовой методы, в рамках которого были оценены отдельные аспекты международного и регионального регулирования киберпреступности. Эмпирическую основу статьи составляют нормативно-правовые акты и акты рекомендательного характера в сфере обеспечения международной информационной безопасности, а также юридическая доктрина, посвященная проблемам указанной отрасли. Выявленные результаты сводятся к следующему: принятие анализируемого международного договора является итогом балансирования противоположных позиций участников переговорного процесса относительно необходимости универсального регулирования кибербезопасности и озабоченности государств риском нарушения прав человека. Установлено, что, несмотря на преодоление спорных вопросов, Конвенция содержит существенные недостатки: высокая вероятность быстрой утраты актуальности вследствие сложности внесения изменений, риск расширительного толкования отдельных положений, что препятствует унификации практики, и в особенности отсутствие эффективного контрольного механизма для мониторинга исполнения обязательств. Автор приходит к выводу о важности принятия Конвенции, ставшей первым универсальным международным договором в области обеспечения международной информационной безопасности, отмечая при этом недостатки Конвенции и правовые риски, связанные со вступлением документа в силу.

Ключевые слова

международная информационная безопасность, киберпреступность, универсальное регулирование, информация, международный договор

Конфликт интересов Автор сообщает об отсутствии конфликта интересов.

Финансирование Исследование не имеет спонсорской поддержки.

Для цитирования Божко, Л. В. (2025). Конвенция ООН против киберпреступности: история и правовые перспективы. *Цифровое право*. https://doi.org/10.38044/2686-9136-2025-6-11

Поступила: 25.07.2025; принята в печать: 15.09.2025

ARTICLES

UN CONVENTION AGAINST CYBERCRIME: HISTORY AND LEGAL PROSPECTS

Lada V. Bozhko[1,2]

[1]Moscow State Institute of International Relations (MGIMO-University)
76, Vernadsky Ave., Moscow, Russia, 119454

[2]Raiffeisenbank
28, Smolenskaya-Sennaya Sq., Moscow, Russia, 119002

Abstract

As a result of the rapid development of information technology and associated increase in cybercrime, the need to ensure international information security has become a critical challenge for the global community. This article analyzes the prospects of the UN Convention against Cybercrime adopted on 24 December 2024 as a mechanism for coordinating the efforts of states in the field of international information security. The aim was to evaluate this international treaty as a basis for cooperation between states in the field of international information security and combating cybercrime. Particular attention is paid to the provisions of the Convention concerning the obligation of states to criminalize the list of acts established by the treaty, as well as ensuring human rights compliance in connection with its application. In the course of the study, the author used historical-legal, formal-legal, and comparative-legal methods to assess certain aspects of international and regional regulation of cybercrime. The empirical basis of the article comprises normative legal acts and those of a recommendatory nature in the field of international information security, as well as legal doctrine devoted to the problems of this industry. The findings can be summarized as follows: the adoption of the international treaty under analysis is an attempt to balance the opposing positions of the participants in the negotiation process regarding the need for universal regulation of cybersecurity with concerns about human rights violations. While the Convention sets out to resolve controversial issues, several significant shortcomings are identified, including a high probability of quickly becoming obsolete due to the complexity of carrying out amendments and the risk of permitting the broad interpretation of certain provisions, which hinders the unification of practice. In particular, the Convention lacks an effective control mechanism for monitoring the fulfilment of obligations. While noting these shortcomings and associated legal risks, the Convention represents the first universal international treaty in the field of international information security and can be recommended for adoption into force.

Keywords
international information security, cybercrime, universal regulation, information, international treaty

Conflict of interest	The author declares no conflict of interest.
Financial disclosure	The study has no sponsorship.
For citation	Bozhko, L. V. (2025). The UN Convention against Cybercrime: History and legal prospects. *Digital Law Journal*. https://doi.org/10.38044/2686-9136-2025-6-11

Submitted: 25 July 2025, accepted: 15 Sept. 2025

Введение

На современном этапе развития общества ключевая роль принадлежит информации. В связи с беспрецедентным ростом ее значения в современном мире необходимо уделять внимание всем аспектам ее использования. Цифровизация и развитие информационно-коммуникационных технологий породили множество угроз и вызовов для международного сообщества. В связи со сложной геополитической ситуацией особое значение приобретает использование информационного пространства в террористических целях, в целях разжигания межгосударственных конфликтов, вмешательства во внутренние дела государств посредством информационных кампаний, кибератак, мошенничества и т.д. Так, отмечается, что «технологии дезинформации активно использовались при подготовке вооруженных вторжений в Югославию (1999 г.), в Ирак (2003 г.), в Ливию (2011 г.) и в Сирию (2016 г.)» (Krutskikh et al., 2021, p. 18).

Вызовы, возникающие в связи с цифровизацией, носят транснациональный характер и требуют реакции как на национальном, так и на двустороннем и универсальном уровнях. Именно с этой целью 24 декабря 2024 г. была принята Конвенция Организации Объединенных Наций против киберпреступности[1]. Данный документ был воспринят неоднозначно и получил широкое обсуждение преимущественно в зарубежной доктрине: вопросам международной информационной безопасности и, в частности, роли данного международного договора в ее обеспечении посвящены работы таких авторов, как А. Ассаф (Assaf, 2023), Э. Шер-Цагир (Scher-Zagier, 2024). Среди отечественных авторов особое внимание Конвенции уделила Д. Д. Штодина (Shtodina, 2025). Так, актуальность настоящего исследования обосновывается неоднозначностью роли принятой Конвенции в области регулирования вопросов международной информационной безопасности и ростом транснациональных киберугроз (Gorelik, 2022, p. 32). Гипотеза исследования заключается в том, что, несмотря на значимость анализируемой Конвенции как первого шага

[1] Полное название конвенции — 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. См.: U.N. Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Dec. 24, 2024, U.N. Doc. A/RES/79/243, https://docs.un.org/ru/A/RES/79/243

к установлению универсального регулирования, этот документ не станет окончательным решением комплексных проблем международной информационной безопасности. Его ограниченная эффективность обусловлена сохраняющимися фундаментальными разногласиями государств — участников переговорного процесса.

История развития регулирования в области обеспечения международной информационной безопасности

Ключевой характеристикой существующего универсального регулирования в сфере международной информационной безопасности является рекомендательный характер принимаемых актов.

Основным регулятором выступает ООН, в рамках деятельности которой были приняты резолюции (в частности, резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» от 5 декабря 2018 г. № 73/27[2] и «Противодействие использованию информационно-коммуникационных технологий в преступных целях» от 17 декабря 2018 г. № 73/187[3]) и доклады Генерального секретаря (на ту же тему от 19 июля 2016 г. A/71/172[4], от 11 августа 2017 г. 72/315[5]).

Среди международных организаций, которые предпринимали шаги по решению проблемы информационной безопасности на региональном уровне, следует также выделить Совет Европы, в рамках которого была принята Конвенция о преступности в сфере компьютерной информации (Будапешт, 23 ноября 2001 г.)[6] (далее — Будапештская конвенция). Среди недостатков данной конвенции особо подчеркивались положения ст. 32, позволяющие одной из сторон конвенции без согласия другой стороны получать доступ к ее компьютерным данным, а также несоответствие документа актуальным тенденциям и вызовам в области информационной безопасности[7].

Попытки ответить на вызовы цифровизации гармонизированным регулированием предпринимались также в рамках Содружества Независимых Государств[8], Организации Договора

[2] G.A. Res. 73/27 (Dec. 5, 2018), https://docs.un.org/ru/A/RES/73/27

[3] G.A. Res. 73/187 (Dec. 17, 2018), https://docs.un.org/ru/A/RES/73/187

[4] U.N. Secretary-General, *Developments in the field of information and telecommunications in the context of international security,* U.N. Doc. A/71/172 (July 19, 2016), https://docs.un.org/ru/A/71/172

[5] U.N. Secretary-General, *Developments in the field of information and telecommunications in the context of international security,* U.N. Doc. A/73/315 (Aug. 11, 2017), https://docs.un.org/ru/A/72/315

[6] Convention on Cybercrime, Mar. 1, 2002, ETS No. 185, 2296 U.N.T.S. 167, https://treaties.un.org/doc/Publication/UNTS/Volume%202296/v2296.pdf. См. неофициальный перевод: https://rm.coe.int/1680081580

[7] Толстухина, А. (2023, 14 сентября). *Российские инициативы в сфере международной информационной безопасности.* Российский Совет по международным делам. https://russiancouncil.ru/analytics-and-comments/analytics/rossiyskie-initsiativy-v-sfere-mezhdunarodnoy-informatsionnoy-bezopasnosti/?sphrase_id=126850521

[8] См., например: Совет глав государств Содружества Независимых Государств, Решение о Концепции сотрудничества государств — участников Содружества Независимых Государств в сфере обеспечения информационной безопасности и о Комплексном плане мероприятий по её реализации на период 2008–2010 годов (10 октября 2008 г.); Соглашение о сотрудничестве государств — участников Содружества Независимых Государств в области обеспечения информационной безопасности (20 ноября 2013 г.), http://publication.pravo.gov.ru/Document/View/0001201506040007?index=1

о коллективной безопасности[9], БРИКС[10], Шанхайской организации сотрудничества[11], Организации по безопасности и сотрудничеству в Европе[12], Регионального форума Ассоциации государств Юго-Восточной Азии по безопасности[13] и «Группы восьми»[14].

Российская Федерация играет важнейшую роль в развитии регулирования в сфере информационной безопасности на универсальном уровне. Первым шагом в этом направлении стало письмо Постоянного представителя РФ при Организации Объединенных Наций на имя Генерального секретаря от 23 сентября 1998 г. (Boyko, 2023, p. 8), в котором было обращено внимание на необходимость предотвращения конфронтации в информационной среде. Затем Российская Федерация в декабре 1998 г. в Первом комитете Генеральной Ассамблеи ООН предложила проект резолюции «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности»[15], положивший начало практике ежегодных резолюций Генеральной Ассамблеи по данному вопросу.

Большой вклад в решение проблемы обеспечения международной информационной безопасности был внесен в рамках переговорных механизмов. Среди них Группа правительственных экспертов, начавшая работу в 2004 г. Результаты ее деятельности выразились в принятии докладов, посвященных анализу возможных угроз в международном информационном пространстве и способов их устранения: 2010[16],

[9] См., например, Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области разработки, производства, эксплуатации, ремонта, модернизации, продления сроков эксплуатации и утилизации продукции военного назначения (10 декабря 2010 г.), http://pravo.gov.ru/proxy/ips/?doc_itself=&backlink=1&nd=201079109&page=1&rdk=0#I0; Соглашение о сотрудничестве государств — членов Организации Договора о коллективной безопасности в области обеспечения информационной безопасности (Минск, 30 ноября 2017 г.), http://publication.pravo.gov.ru/document/0001201904260001?index=1

[10] См., например, BRICS, Sanya Declaration of 14 April 2011, https://brics.br/pt-br/documentos/acervo-de-presidencias-anteriores/leaders-declarations/2011-iii-bric-summit-sanya-declaration.pdf/@@download/file; BRICS, Johannesburg Declaration of 26 July 2018, https://brics.br/pt-br/documentos/acervo-de-presidencias-anteriores/leaders-declarations/2018-x-brics-summit-johannesburg-declaration.pdf/@@download/file

[11] См., например, Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, 16 июня 2009 г., Бюллетень международных договоров январь 2012, № 1, С. 13–21; Циндаоская декларация Совета глав государств-членов Шанхайской организации сотрудничества, 10 июня 2018 г., https://rus.sectsco.org/images/07e8/0b/1b/1603039.pdf

[12] См., например, Org. for Sec. & Co-operation in Eur. [OSCE], *Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, OSCE Doc. PC.DEC/1202 (Mar. 10, 2016), https://www.osce.org/sites/default/files/f/documents/d/a/227281.pdf; OSCE, *Efforts Related to Reducing the Risks of Conflict Stemming from the Use of Info. & Commc'n Tech,* OSCE Doc. MC.DEC/5/16 (Dec. 9, 2016), https://www.osce.org/sites/default/files/f/documents/2/8/288086.pdf

[13] См., например, Ass'n of Se. Asian Nations [ASEAN] & Russian Fed'n, Statement on Cooperation in the Field of Security of and in the Use of Info. & Commc'n Techs. (Nov. 14, 2018), https://asean.org/wp-content/uploads/2018/11/FINAL-Statement-of-ASEAN-and-the-Russian-Federation-on-Cooperation-in-the-Field-of-Security-of-and-in-the-Use-of-Information-and-Communication-Technologies.pdf

[14] См., например, Group of Eight [G8], Okinawa Charter on the Global Info. Soc'y (July 21, 2000).

[15] Russian Federation: draft resolution Developments in the field of information and telecommunications in the context of international security. U.N. Doc. A/C.1/56/L.3 (October 15, 2001), https://docs.un.org/ru/a/c.1/56/l.3

[16] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 30 July 2010 from the Secretary-General. U.N. Doc. A/65/201 (July 30, 2010), https://docs.un.org/ru/A/65/201

2013[17], 2015[18] и 2021[19] гг. Еще одной важной площадкой для решения проблем в области международной информационной безопасности является Рабочая группа открытого состава ООН по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-телекоммуникационных технологий (далее — РГОС), созванная по инициативе Российской Федерации.

Существующий уровень регулирования наглядно демонстрирует острую необходимость создания юридически обязывающего многостороннего международного договора, который сможет закрепить минимальные стандарты защиты на основе выработанной единообразной практики государств и будет отвечать актуальным вызовам в данной области.

В этой связи 27 декабря 2019 г. Генеральной Ассамблеей ООН была принята Резолюция № 74/247 «Противодействие использованию информационно-коммуникационных технологий в преступных целях», согласно которой Генеральная Ассамблея постановила «учредить специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях»[20].

Именно с этой целью на 77-й сессии Генеральной Ассамблеи ООН Российская Федерация предложила обновленную концепцию конвенции Организации Объединенных Наций по международной информационной безопасности (далее — Концепция)[21]. Соавторами инициативы выступили Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа и Сирийская Арабская Республика.

Предложенная в 2023 г. инициатива стала уже третьей попыткой Российской Федерации разрешить дискуссию об установлении регулирования международной информационной безопасности на универсальном уровне.

Впервые проект конвенции Организации Объединенных Наций по международной информационной безопасности Российская Федерация представила 22 сентября 2011 г. В рамках него предлагалось установить основные принципы обеспечения международной информационной безопасности. Несмотря на то, что в документе отмечалась приверженность принципам, закрепленным в международных договорах о правах человека, и сами положения не затрагивали национальный уровень регулирования, а лишь определяли общий вектор действий государств в области обеспечения международной информационной безопасности, проект был подвергнут критике со стороны стран Запада по причине

[17] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 24 June 2013 from the Secretary-General. U.N. Doc. A/68/98* (June 24, 2013), https://undocs.org/ru/a/68/98

[18] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 22 July 2015 from the Secretary-General. U.N. Doc A/70/174 (July 22, 2015), https://docs.un.org/ru/a/70/174

[19] Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, transmitted by Note dated 14 July 2021 from the Secretary-General. U.N. Doc A/70/174 (July 14, 2021), https://docs.un.org/ru/a/76/135

[20] G.A. Res. 74/247, at 3 (Dec. 27, 2019), https://docs.un.org/ru/A/Res/74/247

[21] Updated Concept for a Convention of the United Nations on Ensuring International Information Security, Letter dated May 15, 2023 from the Permanent Representatives of Belarus, the Democratic People's Republic of Korea, Nicaragua, the Russian Federation and the Syrian Arab Republic to the United Nations addressed to the Secretary-General, U.N. Doc. A/77/894 (May 16, 2023), https://docs.un.org/ru/A/77/894

возможного установления им чрезмерного контроля государства над информационным пространством[22].

Следующим шагом в данном направлении стал предложенный Российской Федерацией 11 октября 2017 г. проект конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности[23]. Инициатива охватывает аспекты криминализации и правоохранительной деятельности, а также общие принципы международного сотрудничества и взаимной помощи в области предупреждения и противодействия противоправным деяниям в информационном пространстве. Отличительной чертой данной инициативы можно считать закрепление обязательств государств установить во внутреннем законодательстве ответственность за ряд перечисленных в проекте деяний, среди которых, например, неправомерный доступ к информации в электронной форме, незаконный оборот устройств, сбор информации в электронной форме путем введения пользователя в заблуждение.

Российской Федерацией также был представлен проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях от 29 июня 2021 г.[24] Данный проект также подчеркивает приверженность принципу уважения прав и свобод человека, а также принципу суверенитета государств, в частности в киберпространстве. Инициатива предлагает закрепить обязательства государств по криминализации 23 деяний, среди которых, в частности, незаконное распространение фальсифицированных лекарственных средств и медицинских изделий, преступления, связанные с распространением наркотических средств и психотропных веществ, подстрекательство к подрывной или вооруженной деятельности и т. д.

Впрочем, предлагаемые инициативы не были приняты в качестве основы для международного договора в рамках ООН. Указанные проекты подвергались критике со стороны иных государств — участников ООН, в частности по причине риска широкого толкования положений, что может нанести ущерб законной деятельности журналистов и других лиц, работающих в сфере информации и связи, а также повлечь иные нарушения прав человека[25].

В свою очередь в ранее упомянутой нами обновленной Концепции были сохранены основные принципы предыдущих инициатив, однако документ подвергся изменениям в связи с активной критикой его положений. Важнейшим достижением инициатив Российской Федерации является приверженность единообразной практике, выработанной государствами. Так, Концепция основана на «рекомендациях ежегодных резолюций Генеральной Ассамблеи ООН "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности", а также консенсусных докладов профильной Рабочей группы открытого состава

---

22 Черненко, Е. (2023, 21 мая). Третья пошла. Россия внесла на рассмотрение ООН новый проект конвенции по международной информационной безопасности. Коммерсантъ. https://www.kommersant.ru/doc/5999161

23 Draft United Nations Convention on Cooperation in Combating Cybercrime, in Letter dated Oct. 11, 2017 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. Doc. A/C.3/72/12* (Oct. 16, 2017), https://docs.un.org/en/A/C.3/72/12

24 Ad Hoc Комитет ООН по разработке Конвенции против киберпреступности. (2021, 29 июня). *Проект конвенции Организации Объединенных Наций о противодействии использованию информационно-коммуникационных технологий в преступных целях.* https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_R.pdf

25 Office of the High Commissioner on Human Rights. (2022, January 17). *Key-messages Relating to a Possible Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.* United Nations. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/OHCHR_17_Jan.pdf

(РГОС) ООН 2021 года и групп правительственных экспертов 2010, 2013, 2015 и 2021 годов»[26]. Кроме того, она содержит ссылки на акты, выработанные как на универсальном, так и на региональном уровнях.

Целью конвенции, согласно проекту, является формирование «системы обеспечения международной информационной безопасности на основе равноправного сотрудничества между государствами в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий»[27].

Концепция предлагает закрепить принципы предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве, стремление к развитию сотрудничества в области обеспечения международной информационной безопасности и содействию наращиванию потенциала государств в данной области.

Достоинством Концепции является также положение о необходимости создания механизмов контроля за исполнением государствами положений конвенции, а также механизмов урегулирования и разрешения споров. В качестве образца предлагаются «постоянно действующие органы с участием всех государств, присоединившихся к конвенции, либо обзорные конференции, созываемые на регулярной основе»[28].

Несмотря на высокий уровень разработанности документа, нужно отметить ряд недостатков. В первую очередь к недостаткам Концепции следует отнести низкий уровень конкретизированности и «мягкость» обязательств. Критика предыдущих проектов конвенции на международной арене привела к отказу от закрепления четких обязательств государств, в частности по криминализации определенных деяний. С учетом сложной геополитической ситуации такой шаг был необходим, однако он привел к отдалению от первоначально поставленной цели — создания юридически обязывающего международного договора, который приведет к формированию эффективного универсального регулирования. Во вторую очередь недостатком Концепции является узкий круг ее потенциальных участников: среди соавторов Российской Федерации Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа, Сирийская Арабская Республика. Государства, играющие ключевую роль в обеспечении международной информационной безопасности, являются противниками Концепции.

Анализ Конвенции ООН против киберпреступности

Финалом дискуссии вокруг проекта конвенции стало принятие Резолюцией Генеральной Ассамблеей от 24 декабря 2024 г. 79/243 Конвенции Организации Объединенных Наций против киберпреступности[29]. На 25 августа 2025 г. Конвенция еще не начала действовать, поскольку в соответствии со ст. 65(1) дата вступления ее в силу привязана к дате сдачи на хранение

[26] Updated concept for a convention of the United Nations on ensuring international information security, in Letter dated May, 15 2023 from the Permanent Representatives of Belarus, the Democratic People's Republic of Korea, Nicaragua, the Russian Federation and the Syrian Arab Republic to the United Nations addressed to the Secretary-General, U.N. Doc. A/77/894 (May 16, 2023), https://docs.un.org/ru/A/77/894

[27] Ibid.

[28] Ibid.

[29] U.N. Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Dec. 24, 2024, U.N. Doc. A/RES/79/243, https://docs.un.org/ru/A/RES/79/243

40-й ратификационной грамоты или документа о принятии, утверждении или присоединении[30]. Можно отметить риск невступления Конвенции в силу в связи с обилием противоречий, связанных с текстом и объектом документа. Предметом споров, в частности, стало и название Конвенции. Вариант, принятый Резолюцией, стал своего рода компромиссом, объединив широкий круг преступлений, совершаемых с использованием информационно-коммуникационных систем, а также отразив фокус на киберпреступности, за который выступали оппоненты Российской Федерации в дискуссии вокруг текста Конвенции[31].

Вопрос названия связан с охватом Конвенцией деяний, которые государства-участники должны будут криминализировать в результате присоединения к документу. Как было упомянуто ранее, Российская Федерация предлагала 23 состава, тогда как финальная версия Конвенции содержит лишь одиннадцать:

1) незаконный доступ;
2) незаконный перехват;
3) воздействие на электронные данные;
4) воздействие на информационно-коммуникационную систему;
5) неправомерное использование устройств;
6) подлог с использованием информационно-коммуникационной системы;
7) хищение или мошенничество с использованием информационно-коммуникационной системы;
8) преступления, связанные с размещением в Интернете материалов со сценами сексуальных надругательств над детьми или их сексуальной эксплуатации,
9) домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка;
10) распространение интимных изображений без согласия; и
11) отмывание доходов от преступлений.

При этом возможность дальнейшего расширения перечня осложняется не только разнополярностью позиций договаривающихся государств, но и тем, что обязательным требованием для принятия дополнительного протокола является наличие не менее 60 государств — участников договора. Не менее труднореализуема и процедура внесения поправок, которая предполагает истечение пяти лет после вступления Конвенции в силу. Следует также отметить, что особенностью сферы информационной безопасности является быстрота изменений, в связи с чем сложность внесения поправок и длительные сроки особенно ощутимы для обеспечения эффективности регулирования.

Помимо сокращения перечня криминализируемых деяний, в юридической доктрине выделяют также иные недостатки Конвенции. Так, Д. Д. Штодина в качестве лакун документа указывает вопросы реализации пассивного персонального принципа установления юрисдикции и защиты персональных данных пользователей Интернета (Shtodina, 2025, p. 118). Согласно пассивному персональному принципу определяющим фактором для установления государством

---

30 U.N. Convention against Cybercrime, art. 65, ¶ 1.

31 Черненко, Е. (2024, 30 июля). Киберчувствительная тема. Проект конвенции ООН по борьбе с компьютерной преступностью не нравится ни России, ни ее оппонентам. *Коммерсантъ*. https://www.kommersant.ru/doc/6864552?query=%D0%9A%D0%BE%D0%BD%D0%B2%D0%B5%D0%BD%D1%86%D0%B8%D1%8F%20%D0%BF%D0%BE%20%D0%BC%D0%B5%D0%B6%D0%B4%D1%83%D0%BD%D0%B0%D1%80%D0%BE%D0%B4%D0%BD%D0%BE%D0%B9%20%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D0%BE%D0%B9%20%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8

юрисдикции является гражданство жертвы преступления. В ходе переговорного процесса Российская Федерация, а также Иран, Кабо-Верде, Пакистан, Панама, Эритрея и Сирия предлагали распространить данный принцип также на случаи совершения противоправных деяний в отношении юридических лиц, учрежденных или имеющих постоянное представительство на территории государства, устанавливающего свою юрисдикцию. Возможность установления данного принципа в отношении преступлений против международной информационной безопасности была раскритикована в связи с риском расширительного толкования, вызванным отсутствием в Конвенции ограничений данного положения (Scher-Zagier, 2024, p. 366). Тогда как Комиссия международного права в отчете от 2006 года[32] пришла к выводу о том, что на национальном уровне государства ограничивают область применения пассивного персонального принципа перечнем наиболее тяжких преступлений, среди которых, в частности, терроризм. Среди иных ограничительных условий также применяется требование двойной криминализации, применение данного принципа только в отношении преступлений, предусматривающих минимальную меру наказания (Watson, 1993, p. 23), отказ государства, которое могло бы установить свою юрисдикцию на основании территориального принципа (McCarthy, 1989, p. 24).

Необходимо отметить, что положение о возможности применения пассивного персонального принципа было основано на аналогичной норме Конвенции ООН против транснациональной организованной преступности (принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года[33]) (далее — Конвенция против транснациональной организованной преступности)[34], и Конвенции ООН против коррупции (принята резолюцией 58/4 Генеральной Ассамблеи от 31 октября 2003 года[35]) (далее — Конвенция против коррупции)[36]. Для конференций государств-участников анализируемых конвенций функции секретариата выполняет Управление Организации Объединенных Наций по наркотикам и преступности (далее — УНП ООН), которое при разработке Конвенции против киберпреступности подготовило обзор существующих источников правового регулирования в области обеспечения международной информационной безопасности[37], при этом включив туда как Конвенцию против транснациональной организованной преступности, так и Конвенцию против коррупции, отмечая, однако, что объектом их регулирования являются иные правоотношения. Так, статья 15 Конвенции против транснациональной организованной преступности закрепила возможность государств установить свою юрисдикцию в отношении любого преступления, которое совершено против гражданина этого государства[38]. Конвенция против коррупции в статье 42 также устанавливает возможность применения принципа пассивной юрисдикции, не закрепляя при этом ограничительных условий[39]. США, комментируя выбор Конвенции против коррупции в качестве основы для раз-

[32] Report of the International Law Commission to the General Assembly, 2006, U.N. GAOR Supp. No. 10, at 524 n. 23, U.N. Doc. A/61/10.

[33] G.A. Res. 55/25, United Nations Convention Against Transnational Organized Crime (Nov. 15, 2000).

[34] United Nations Convention Against Transnational Organized Crime, Nov. 15, 2000, 2225 U.N.T.S. 209.

[35] G.A. Res. 58/4, United Nations Convention Against Corruption (Oct. 31, 2003).

[36] United Nations Convention Against Corruption, Oct. 31, 2003, 2349 U.N.T.S. 41.

[37] United Nations Office on Drugs and Crime Secretariat, Overview of Existing Instruments, Recommendations and Other Documents on Countering the Use of Information and Communications Technologies for Criminal Purposes, Apr. 20, 2022, U.N. Doc. A/AC.291/CRP.10.

[38] United Nations Convention Against Transnational Organized Crime, art. 15.

[39] United Nations Convention Against Corruption, art. 42.

работки универсального источника регулирования проблемы обеспечения международной информационной безопасности, отмечали, что процесс разработки данного международного договора был более длительным и был инициирован на основе консенсуса государств, чего в данном случае нет[40].

При этом Э. Шер-Цагир отмечает, что Конвенция против транснациональной организованной преступности и Конвенция против коррупции все же представляют собой пример ограничительного использования пассивного персонального принципа. Так, объект регулирования Конвенции против транснациональной организованной преступности предполагает наличие таких ограничительных условий как определенная структура, период действия и цель преступных групп. Возможность применения пассивного персонального принципа в соответствии с Конвенцией против коррупции может рассматриваться как частное проявление защитного принципа установления юрисдикции, поскольку объект ее регулирования тесно связан с ключевыми интересами государства (Scher-Zagier, 2024, p. 364).

Данный принцип установления юрисдикции становится предметом критики не в первый раз. Так, Седрик Рейнгарт утверждает, что данный принцип установления юрисдикции не выполняет сдерживающей, превентивной функции, являющейся основной в уголовном праве. Это объясняется тем, что преступник не может предвидеть, какое государство установит юрисдикцию, поскольку он будет обычно не знает национальности жертвы (Ryngaert, 2015, p. 110). Еще Доннедье де Вабр подчеркивал, что применение принципа пассивной персональной юрисдикции лишь усиливает противоречия государств по вопросам установления юрисдикции (Donnedieu de Vabres, 1928, p. 170).

Однако критика использования пассивного персонального принципа представляется недостаточно обоснованной. Данный принцип не противоречит превентивной функции уголовного права, поскольку она связана в первую очередь с наличием ответственности за совершенное противоправное деяние, а невозможность спрогнозировать формы ее реализации может служить лишь дополнительным усиливающим сдерживающий характер фактором. При этом, интерес государства гражданства жертвы представляется обоснованным и правомерным, поскольку является следствием факта нарушения прав его гражданина. Что касается ограничительных условий применения пассивного персонального принципа, Конвенция против киберпреступности в качестве обязательств государств-участников устанавливает криминализацию указанных в ней деяний, что представляет собой требование двойной криминализации, являющееся одним из проявлений ограничительных условий[41]. Кроме того, перечень деяний, которые государства должны признать в качестве уголовного правонарушения в соответствии с Конвенцией против киберпреступности, является ограниченным и не может толковаться расширительно. Наличие таких ограничительных положений, а также закрепленное в договоре требование выполнения обязательств в соответствии с принципами суверенного равенства и территориальной целостности государств и принципом невмешательства во внутренние дела других государств[42] позволяют сделать вывод о чрезмерности опасений противников применения такого принципа.

---

40 United States of America, "Implementation of Operative Paragraph 3 of General Assembly Resolution 74/247 and Next Steps", Apr. 20, 2020, U.N. Doc. A/AC.291/CRP, (Ad Hoc Comm. to Elaborate a Comprehensive Int'l Convention on Countering the Use of ICTs for Criminal Purposes), available at https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/USA.pdf

41 U.N. Convention against Cybercrime, art. 7–17.

42 Ibid., art. 5.

Что касается защиты персональных данных, предметом критики выступили положения Конвенции о сборе доказательств: предлагалось закрепить возможность передачи данных только «в случае наличия серьезных оснований полагать, что преступление носит "серьезный характер"» (Shtodina, 2025, p. 122). Однако необходимо отметить, что существующая в Конвенции формулировка, позволяющая сбор доказательств по уголовным правонарушениям в соответствии с Конвенцией[43], решает проблему Будапештской конвенции, закрепляющей возможность доступа к данным без согласия другой стороны[44]. Соответствующее положение Будапештской конвенции с точки зрения отечественной доктрины «фактически представляет собой норму, регламентирующую не что иное, как обыск в компьютерных сетях (или в среде для хранения компьютерных данных) за рубежом с целью обнаружения и изъятия искомой компьютерной информации» (Volevodz, 2007, p. 25), а также влечет риск нарушения фундаментальных прав и свобод человека в цифровой среде (Danel'yan, 2020, p. 265).

Существенным недостатком Конвенции является отсутствие контрольного механизма, который предлагала закрепить Российская Федерация. С целью эффективного контроля за исполнением положений документа представляется оптимальным создание договорного органа или специальной процедуры Совета по правам человека. В качестве примера эффективно функционирующих договорных механизмов можно привести десять органов ООН по правам человека (Abashidze & Koneva, 2015, p. 14). Среди них, в частности, Комитет по правам ребенка, который наблюдает за выполнением Конвенции о правах ребенка 1989 г.[45] и двух факультативных протоколов к ней, касающихся сексуальной эксплуатации детей, их участия в вооруженных конфликтах, а также торговли детьми[46]. Однако, помимо договорных органов, мониторинг и привлечение внимания к актуальным нарушениям прав человека также может эффективно осуществляться посредством деятельности специальных процедур Совета по правам человека. Так, деятельность специального докладчика по вопросу о рабстве способствовала привлечению внимания международного сообщества к проблеме создания незаконного онлайн-рынка рабского труда крупными технологическими компаниями[47]. Создание подобного механизма в рамках принятой Конвенции против киберпреступности позволило бы отслеживать существующую ситуацию в области международной информационной безопасности, контролировать соблюдение государствами-участниками Конвенции и выявлять соответствующие нарушения.

В зарубежной доктрине Конвенция подверглась критике преимущественно в части положений, посвященных международному сотрудничеству (Tropina, 2024, p. 220; Tennant & Oliveira, 2024, p. 238). Так, К. Родригес характеризует данную главу документа как «главу о трансграничном шпионаже» и отмечает, что сфера действия статьи 24 Конвенции, устанавливающей обязанность государств обеспечивать защиту прав человека и действовать в соответствии с принципом соразмерности[48], ограничивается областью применения процессуальных мер

[43] U.N. Convention against Cybercrime, art. 23.

[44] Convention on Cybercrime, art. 32(b), Mar. 1, 2002, ETS No. 185, 2296 U.N.T.S. 167, https://treaties.un.org/doc/Publication/UNTS/Volume%202296/v2296.pdf

[45] Convention on the Rights of the Child, Nov. 20, 1989, 1577 U.N.T.S. 3.

[46] *See,* Optional Protocol to the Convention on the Rights of the Child on the Involvement of Children in Armed Conflict, May 25, 2000, 2173 U.N.T.S. 222; Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, May 25, 2000, 2171 U.N.T.S. 227.

[47] Совет по правам человека. (б.д.). *Результаты работы Специальных процедур: предупреждение и/или прекращение нарушений прав человека.* По обращению 24 июля 2025 к https://www.ohchr.org/ru/special-procedures-human-rights-council/impact-work-special-procedures-prevention-andor-cessation-human-rights-violations

[48] U.N. Convention against Cybercrime, art. 24.

согласно Конвенции и не распространяется на международное сотрудничество государств[49]. Следует подчеркнуть, что данный довод представляется необоснованным: необходимость уважения и защиты прав человека, в том числе в ходе международного сотрудничества государств в рамках исполнения обязательств, вытекающих из Конвенции, закреплена в ст. 6 Конвенции[50]. В ходе переговорного процесса ряд стран, в том числе Новая Зеландия, Вануату, Норвегия и Лихтенштейн, предлагали внести в статью 35 Конвенции, посвященную общим принципам международного сотрудничества[51], положение, которое могло бы стать дополнительной гарантией защиты прав человека[52]. Предложение содержало формулировку, позволяющую государству отказать в исполнении запроса о международном сотрудничестве, если есть веские основания полагать, что такой запрос был сделан с целью преследования или наказания лица по признаку пола, расы, языка, религии, национальности, этнического происхождения или политических убеждений или что выполнение запроса нанесет ущерб положению этого лица по любой из этих причин. Однако указанное предложение не было учтено в финальной редакции Конвенции.

Следует также отметить иной недостаток Конвенции, которому уделяет внимание К. Родригес[53]. Конвенция не содержит определений ключевых для данной сферы понятий: «данные» и «информация». Их отсутствие может повлечь расширительное толкование положений документа, что несет в себе риски для обеспечения надлежащего уровня защиты персональных данных и конфиденциальной информации.

Скорость разработки документа выделяется в качестве одной из причин существующих недостатков Конвенции: поскольку участники переговорного процесса были вынуждены сосредоточить внимание на согласовании наиболее дискуссионных условий договора, ряд положений не был надлежащим образом разработан. Так, Э. Шер-Цагир обращает внимание на процесс разработки анализируемого международного договора: график включал всего семь сессий переговоров менее чем за два года (Scher-Zagier, 2024, p. 346). Так, именно с этим автор связывает проблему применения пассивного персонального принципа установления юрисдикции в соответствии с Конвенцией. Однако мы не можем согласиться с данной позицией, поскольку работа по разработке международного договора в области обеспечения международной информационной безопасности ведется на протяжении длительного периода времени, и разногласия государств обусловлены не недостаточной продолжительностью дискуссий, а концептуальными различиями подходов и конфликтом политических интересов.

На момент написания статьи работа по созданию системы регламентации в области обеспечения международной безопасности продолжается. В Нью-Йорке 7 июля 2025 г. открылась финальная сессия РГОС, по результатам который должен быть подготовлен доклад, отражающий общую позицию международного сообщества в области обеспечения международной

---

[49] Rodriguez, K. (2023, August 22). *Proposed UN Cybercrime Treaty threatens to be an expansive global surveillance pact*. Electronic Frontier Foundation. https://www.eff.org/deeplinks/2023/08/proposed-un-cybercrime-treaty-threatens-be-expansive-global-surveillance-pact

[50] U.N. Convention against Cybercrime, art. 6.

[51] Ibid., art. 35.

[52] Draft text of the convention with the amendments made by Member States. Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. Sixth session. New York, 21 August — 1 September 2023. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf

[53] Rodriguez, K. Op. cit.

информационной безопасности[54]. Работа РГОС приведет к принятию доклада, нового акта рекомендательного характера, лишь косвенно способствуя формированию системы юридически обязывающего регулирования в данной сфере.

Заключение

Таким образом, гипотеза исследования подтвердилась. Конвенция стала первым международным юридически обязывающим актом в сфере международной информационной безопасности, выступая в роли необходимого, но промежуточного этапа, поскольку присущие ей существенные недостатки не позволяют ей полностью решить комплексные вызовы безопасности в динамично развивающемся киберпространстве. Как результат длительной дискуссии, она является компромиссом между позициями Российской Федерации и иных государств, выступающих за необходимость универсального регулирования в данной области, и их оппонентов, которые видят в этом риск нарушения прав человека и злоупотреблений государствами. Несмотря на то, что опасения государств, связанные с возможностью использования документа как инструмента слежки, представляются преувеличенными, принятый в 2024 г. международный договор все же обладает рядом недостатков.

Во-первых, Конвенция отличается трудностью внесения изменений, что, в свою очередь, порождает риск неактуальности положений договора в связи с развитием информационных технологий.

Во-вторых, недостатком является возможность расширительного толкования отдельных положений Конвенции, к числу которых относятся, в частности, отсутствие определений понятий «данные» и «информация» и вопросы сбора доказательств. Вероятно, причина этому — необходимость согласования разнополярных позиций договаривающихся государств. Однако широта формулировок не может считаться решением данной проблемы, поскольку позволяет государствам самостоятельно толковать указанные положения, что препятствует достижению цели Конвенции — закреплению единообразной практики.

В-третьих, существенным недостатком данного международного договора является отсутствие механизмов контроля за исполнением его положений.

В-четвертых, можно поставить под сомнение само вступление Конвенции в силу в связи с необходимостью внесения 40 ратификационных грамот или документов о принятии, утверждении или присоединении на фоне не устраненных до конца противоречий в позициях договаривающихся государств.

Несовершенство Конвенции, продолжительность дискуссий, полярность позиций, обилие критики приводят к возникновению более глобального вопроса, способного послужить предметом отдельного исследования, — о том, каким должно быть регулирование международной информационной безопасности. В результате анализа существующего регулирования можно предположить, что наиболее эффективным путем его развития стало бы сочетание рамочного международного договора и актов рекомендательного характера. Эффективное регулирование недостижимо без закрепления обязательств, что реализуемо именно посредством заключения международного договора. Однако с учетом быстроты изменений в данной сфере представляется невозможным исчерпывающим образом охватить

[54] Черненко, Е. (2025, 7 июля). Цифровую ответственность оформят докладом. На площадке ООН вновь обсудят правила поведения государств в киберпространстве. *Коммерсантъ*. https://www.kommersant.ru/doc/7871382

все требующие регламентации области посредством заключения международного договора. Акты рекомендательного характера представляют собой более гибкий механизм, способный отражать актуальные тенденции отрасли. Так, Конвенция не стала финалом дискуссии о регулировании информационной безопасности на универсальном уровне, но выступила важнейшим шагом в этом направлении.

Список литературы / References

1. Abashidze A. Kh., & Koneva A. E. (2015). *Dogovornye organy po pravam cheloveka: uchebnoe posobie* [Human rights treaty bodies: A study guide] (2nd ed.). RUDN.
2. Assaf, A. (2023). Violations of sovereignty in "cyberspace" under the United Nations Charter. *Zhurnal VSHÉ po Mezhdunarodnomu Pravu* [*HSE University Journal of International Law*], *1*(3), 4–20. https://doi.org/10.17323/jil.2023.18848
3. Boyko, S. M. (2023). Mezhdunarodnaya informatsionnaya bezopasnost': Rossiya v OON. Nachalo istorii (1998-2009 gg.) [International information security: Russia at the United Nations. The beginning of the story (1998–2009)]. *Mezhdunarodnaya Zhizn'*, (11), 8–23.
4. Danel'yan, A. A. (2020). Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International legal regulation of cyberspace]. *Obrazovanie i Pravo*, (1), 261–269. https://doi.org/10.24411/2076-1503-2020-10140
5. Donnedieu de Vabres, H. (1928). *Les principes modernes du droit pénal international* [Modern principles of international criminal law]. Librairie du Recueil Sirey.
6. Gorelik, I. B. (2022). Rol' mezhdunarodnykh organizatsiy v protsesse protivodeystviya kiberprestupnosti [The role of international organizations in the process of countering cybercrime]. *Mezhdunarodnoe Pravo*, (3), 28–41. https://doi.org/10.25136/2644-5514.2022.3.38585
7. Krutskikh, A. V., Biryukov A. V., Boyko, S. M., Volkova, S. G., Zinovieva, E. S., Zinchenko, A. V., Matyukhin, D. V., & Smirnov, A. I. (2021). *Mezhdunarodnaya informatsionnaya bezopasnost': Teoriya i praktika: Uchebnik v trekh tomakh. T. 2.* [*International information security: Theory and practice: Textbook* (Vol. 2; 2nd ed.)]. Aspekt Press.
8. McCarthy, J. G. (1989). The passive personality principle and its use in combatting international terrorism. *Fordham International Law Journal*, *13*(3), 298–327.
9. Ryngaert, C. M. J. (2015). *Jurisdiction in international law* (2nd ed.). Oxford University Press.
10. Scher-Zagier, E. (2025). Jurisdictional creep: The UN Cybercrime Convention and the expansion of passive personality jurisdition. *Yale Journal of Law & Technology, 27*(1), 327–389.
11. Shtodina, D. D. (2025). Konventsiya Organizatsii Ob'yedinennykh Natsiy protiv kiberprestupnosti 2024 goda — itog "kiberkompromissa"? [United Nations Convention against Cybercrime, 2024 — the outcome of «cyber compromise»?] *Moskovskij Zhurnal Mezhdunarodnogo Prava*, (1), 110–124. https://doi.org/10.24833/0869-0049-2025-1-110-124
12. Tennant, I., & Oliveira, A. P. (2024). Applying the right lessons from the negotiation and implementation of the UNTOC and the UNCAC to the implementation of the newly agreed UN 'cybercrime' treaty. *Journal of Cyber Policy*, *9*(2), 221–238. https://doi.org/10.1080/23738871.2024.2428655
13. Tropina T. (2024). 'This is not a human rights convention!': The perils of overlooking human rights in the UN cybercrime treaty. *Journal of Cyber Policy*, *9*(2), 200–220. https://doi.org/10.1080/23738871.2024.2419517
14. Volevodz, A. G. (2007). Konventsiya o kiberprestupnosti: novatsii pravovogo regulirovaniya [The Convention on cybercrime: Innovations in legal regulation]. *Pravovye Voprosy Svyazi*, (2), 17–25.
15. Watson, G. R. (1993). The passive personality principle. *Texas International Law Journal*, *28*(1), 1–46.

Сведения об авторе:

Божко Л. В. — магистрант, международно-правовой факультет, МГИМО МИД России, юрист отдела сопровождения корпоративного бизнеса и банковской деятельности, АО «Райффайзенбанк», Москва, Россия.
lada-bozhko@mail.ru
ORCID: https://orcid.org/0009-0002-2637-170X

Information about the author:

Lada V. Bozhko — Master's student, International Law Faculty, Moscow State Institute of International Relations, lawyer in the Corporate Business and Banking Support Department, Raiffeisenbank JSC, Moscow, Russia.
lada-bozhko@mail.ru
ORCID: https://orcid.org/0009-0002-2637-170X