DOI: https://doi.org/10.24833/0869-0049-2025-1-110-124

Исследовательская статья
УДК: 341.1/8
Поступила в редакцию: 10.01.2025
Принята к публикации: 05.03.2025

ШТОДИНА Дарья Дмитриевна
Национальный исследовательский университет «Высшая школа экономики»
Большой Трехсвятительский пер., д. 3, Москва, 109028, Российская Федерация
dashashtodina96@gmail.com
ORCID: 0000-0003-4730-9614

КОНВЕНЦИЯ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ПРОТИВ КИБЕРПРЕСТУПНОСТИ 2024 ГОДА – ИТОГ «КИБЕРКОМПРОМИССА»?

ВВЕДЕНИЕ. *Международно-правовой режим киберпространства сегодня нуждается в дополнительной правовой регламентации, поскольку по некоторым аспектам, в частности, по борьбе с киберпреступностью, до 2024 г. не был принят универсальный международный договор. По мнению автора, искусственное затягивание переговорного процесса обосновывается стремлением ряда государств заблаговременно «осваивать» новую территорию в международном праве, руководствуясь при этом положениями внутреннего нормативно-правового регулирования. Поскольку на уровне Организации Объединенных Наций (далее – ООН) у международного сообщества длительное время не было универсальных «механизмов воздействия» на неправомерную деятельность в киберпространстве, то количество совершаемых киберпреступлений стремительно возрастало, а киберпреступники, в свою очередь, использовали анонимность данного пространства для совершения кибератак. Признание государствами как первичными субъектами международного права проблемы роста кибернетической преступности в отсутствие действующего универсального источника международного права спустя более двадцати лет привело к созданию в 2024 г. нового документа – «Конвенции 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» (далее – Конвенция ООН против киберпреступности 2024 г.). Таким образом, в данной работе исследуется проблема толкования новой Конвенции как итогового и эффективного компромисса, к которому пришли государства.*

МАТЕРИАЛЫ И МЕТОДЫ. *В статье используются работы российских и зарубежных специалистов, исследующих положения Конвенции ООН против киберпреступности 2024 г., а также некоторые теоретические исследования в сфере международного уголовного права, посвященные проблеме применения государствами «принципа активной юрисдикции» и «принципа пассивной юрисдикции». Помимо общенаучных методов исследования (анализ, синтез, индукция и дедукция) автор использует специальные методы исследования (сравнительно-правовой метод) для всестороннего изучения международно-правовой позиции государств по вопросу борьбы с киберпреступностью. Предметом исследования выступают международные отношения государств – членов ООН, связанные с сотрудничеством по пресечению и борьбе с кибернетической преступностью. К объекту исследования отнесена киберпреступность в государствах – членах ООН.*

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ. *В результате исследования были выделены два основных проблемных аспекта реализации положений нового документа: применение «принципа пассивной юрисдикции» и вопрос, связанный с защитой персональных данных пользователей Интернета. Существует вероятность того, что вместо заявленной государствами цели – борьбы с преступностью, основные усилия данных субъектов будут направлены на отстаивание права толковать положения Конвенции против киберпреступности, руководствуясь нормами внутреннего законодательства, сужая при этом возможность конкретному пользователю получить защиту своих прав.*

ОБСУЖДЕНИЕ И ВЫВОДЫ. *Сегодня тенденции изменения международно-правового режима киберпространства диктуются не столько государствами как носителями суверенитета в отношении национального сегмента Интернета, сколько ведущими IT-компаниями и организациями, отстаивающими право на автономное регулирование с минимальным участием первичных субъектов международного права. Несмотря на принятие Генеральной Ассамблеей ООН Конвенции против киберпреступности, не приходится констатировать достижение компромисса, поскольку при составлении текста документа каждое государство по-разному воспринимало его итоговую цель. Некоторые государства скептически относятся к итоговому документу ООН и предпочитают использовать Будапештскую конвенцию 2001 г. как механизм по борьбе с преступлениями в киберпространстве. Основная проблема универсальной Конвенции касается толкования целого ряда положений, затрагивающих проблему применения «принципа пассивной юрисдикции», условий и гарантий соблюдения прав человека в случае привлечения к ответственности по политическим мотивам пользователей, а также возможности сотрудничества США, западных государств по данным вопросам с Россией и Китаем в текущих реалиях.*

КЛЮЧЕВЫЕ СЛОВА: *киберпространство, информационно-коммуникационные технологии, киберпреступность, Конвенция ООН против киберпреступности, «принцип пассивной юрисдикции», защита персональных данных, информационно-коммуникативная система, cyber-enabled crimes, cyber-dependent crimes*

ДЛЯ ЦИТИРОВАНИЯ: Штодина Д.Д. 2025. Конвенция Организации Объединенных Наций против киберпреступности 2024 года – итог «киберкомпромисса»? – *Московский журнал международного права.* № 1. С. 110–124. DOI: https://doi.org/10.24833/0869-0049-2025-1-110-124

Автор заявляет об отсутствии конфликта интересов.

MASS INFORMATION AND INTERNATIONAL LAW

DOI: https://doi.org/10.24833/0869-0049-2025-1-110-124

Research article
UDC: 341.1/8
Received 10 January 2025
Approved 5 March 2025

Daria D. SHTODINA
National Research University Higher School of Economics
3, Bolshoy Tryokhsvyatitelsky Ln., Moscow, Russian Federation, 109028
dashashtodina96@gmail.com,
ORCID: 0000-0003-4730-9614

UNITED NATIONS CONVENTION AGAINST CYBERCRIME, 2024 – THE OUTCOME OF "CYBER COMPROMISE"?

INTRODUCTION. *Today the international legal regime of cyberspace is in need of more accurate, additional regulation, since there are some particular aspects, such as cybercrime, where there is no universal legal source of law (i.e. international treaty). According to the author's opinion, the artificial prolongation of the negotiation process can be justified by the desire of certain states to «master» a new territory of international law in advance, while being guided by the provisions of domestic legal regulation. For a long time the international community at the UN level had no mechanisms of influence on illegal activities in this domain. Thus, the number of cybercrimes committed in cyberspace was rapidly increasing, since cybercriminals resorted to the anonymity of this space. The recognition by states as primary subjects of international law of the growing problem of cybercrimes in the absence of the valid universal source of international law more than twenty years later led to the creation of the United Nations 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, 2024.*

MATERIALS AND METHODS. *This article is based on the references to the works of Russian and foreign specialists studying new provisions of the UN Convention against Cybercrime, 2024, as well as some theoretical issues in the field of international criminal law, devoted to the problem of application by states of the so-called «principle of active jurisdiction» and "principle of passive (personality) jurisdiction". In addition to general, basic research methods such as analysis, synthesis, induction and deduction, the author uses special research methods, such as comparative legal method for a comprehensive study of the international legal position of states on the issue of cybercrime. The subject of this study is international relations of the UN member states related to cooperation in suppressing and combating cybercrimes.*

RESEARCH RESULTS. *As a result of the study, the author identifies two main problematic aspects of the implementation of the document: 1) passive personality jurisdiction, and 2) the issue related to the protection of personal data. There is a probability that instead of the stated goals of the UN member states to fight crimes, committed in cyberspace, the main efforts of these actors will be aimed at the right to construe the provisions of the Convention against Cybercrime, guided by the norms of domestic legislation.*

DISCUSSION AND CONCLUSIONS. *The current legal tendency is that the rules of the legal regime of cyberspace are dictated not only by states as the main subjects of international law, but by leading IT companies and private organizations asserting the right to autonomous regulation with only minimal participation of states as well as international organizations. Despite the fact that the UN Convention against Cybercrimes has been adopted, each state perceived its final goal differently when drafting the text of the document. Some states remain skeptical and suppose that the final convention has certain legal lacunae and thus prefer to use the 2001 Budapest Convention to combat cybercrimes.*

KEYWORDS: *cyberspace, information and communication technologies, cybercrime, UN Convention against Cybercrime, passive personality jurisdiction principle, personal data protection, information and communication system, cyber-enabled crimes, cyber-dependent crimes*

FOR CITATION: Shtodina D.D. United Nations Convention against Cybercrime, 2024 – the Outcome of «Cyber Compromise»? – *Moscow Journal of International Law.* 2025. No. 1. P. 110–124. DOI: https://doi.org/10.24833/0869-0049-2025-1-110-124

The author declares the absence of conflict of interest.

1. Введение: правовые механизмы борьбы с киберпреступностью в рамках ООН

Изучение международно-правовых аспектов сотрудничества в сфере борьбы с киберпреступностью становится все более актуальным [Иноземцев 2021:18-28]. Согласно данным глобального индикатора Estimated Cost of Cybercrime, уровень кибернетической преступности в период с 2024 г. по 2029 г. неизменно будет увеличиваться с каждым годом на 6,4 трлн долл. США (т.е. на 69,41 %)[1].

[1] Statista: Estimated cost of cybercrime worldwide 2018–2029. URL: https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide (accessed date: 10.02.2025).

В основном кибернетические атаки наносят ущерб производителям товаров, крупнейшим финансовым секторам и компаниям, предоставляющим услуги по страхованию. Особенно актуальна проблема создания так называемых программ-вымогателей (ransomware attacks), которые используются киберпреступниками в 70 % случаев[2]. Согласно данным Statista, большая часть компаний стали выделять финансирование на борьбу с кибернетическими атаками. Например, в 2023 г. одним из приоритетов для компаний различных секторов экономики стало повышение устойчивости к киберугрозам посредством увеличения расходов, направленных на борьбу с кибератаками[3].

Правовой режим кибернетического пространства (cyberspace) рассматривается в международном праве в качестве «новой территории», или объекта владения (domain) наряду с другими пространствами, изучаемыми в классическом курсе международного права. Очевидно, что киберпространство по своим «физическим» характеристикам значительно отличается от иных территорий [Данельян 2020:261-269] (например, cyberspace наделено такими чертами, как анонимность, трансграничность, невозможность осуществления централизованного контроля за действиями всех акторов, т.е., прежде всего, IT-гигантов, снижением роли государства в регулировании кибернетического пространства и т.д.) [Khanna 2018:139-154]. Из этого напрямую следует, что подобное пространство, или domain (термин, используемый в американских правовых документах по данной проблематике [Clarke, Knake 2019:320]), становится своеобразным *paradisus* для преступников, искусно пользующихся анонимностью и иными гарантиями конфиденциальности [Комова, Сидоренко 2023:74-85].

На универсальном уровне, в рамках ООН, начало дискуссии о необходимости противодействия киберпреступности и определения правовых рамок для деятельности пользователей и юридических лиц было положено в 2010 г., когда Генеральная Ассамблея ООН (далее – ГА ООН) приняла резолюцию A/65/230, в которой была подчеркнута роль Комиссии по предупреждению преступности и уголовному правосудию как органа, ответственного за выработку и осуществление мер, направленных на создание «… новых национальных и международных правовых или иных мер по противодействию киберпреступности»[4]. Именно на основании данного источника soft law Комиссией по предупреждению преступности и уголовному правосудию в 2011 г. была учреждена Межправительственная группа экспертов открытого состава для проведения всестороннего исследования проблемы киберпреступности (далее – Группа экспертов по киберпреступности).

В 2011 г. Группой экспертов по киберпреступности был подготовлен документ «Проекты тем для рассмотрения в рамках всестороннего исследования проблемы киберпреступности и ответных мер», в котором были выделены четыре источника (или формы) борьбы с киберпреступностью: 1) многосторонние договоры о международном сотрудничестве в борьбе с преступностью; 2) многосторонние договоры о судебном преследовании за определенные преступления; 3) специализированные двусторонние договоры; и 4) национальное законодательство, положения которого могут регулировать механизмы международного сотрудничества в сфере борьбы с киберпреступностью[5]. Примечательно, что Группа экспертов по киберпреступности особо подчеркивала роль частного сектора для осуществления международного кибернетического сотрудничества.

---

[2] Statista: Sectors worldwide frequently affected by industrial ransomware incidents in 2023, by number of attacks. URL: https://www.statista.com/statistics/1368824/industries-targeted-industrial-ransomware-attacks-by-number-of-attacks/ (accessed date: 10.02.2025).

[3] Statista: Areas of priority spending for improving cyber resilience in 2023, by priority level. URL: https://www.statista.com/statistics/1387069/top-spending-priorities-for-cyber-resilience/ (accessed date: 10.02.2025).

[4] ООН: Резолюция, принятая Генеральной Ассамблеей [по докладу Третьего комитета (A/65/457)] 65/230. Двенадцатый Конгресс ООН по предупреждению преступности и уголовному правосудию. URL: https://www.unodc.org/documents/justice-and-prison-reform/AGMs/A_RES_65_230r.pdf (дата обращения: 10.02.2025).

[5] Группа экспертов по киберпреступности: Проекты тем для рассмотрения в рамках всестороннего исследования проблемы киберпреступности и ответных мер. URL: https://www.unodc.org/documents/treaties/organized_crime/EGM_cybercrime_2011/UNODC_CCPCJ_EG4_2011_2/UNODC_CCPCJ_EG4_2011_2_R.pdf (дата обращения: 10.02.2025).

2. Предыстория создания Конвенции ООН по борьбе с киберпреступностью 2024 г.: позиции государств-членов

Современная повестка ООН по противодействию кибернетической преступности будет рассмотрена ниже, возвращаясь к предыстории вопроса отметим, что в 2019 г. на основании резолюции ГА ООН A/74/247 был создан Межправительственный комитет экспертов открытого состава для разработки всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий (далее – ИКТ) в преступных целях (т.е. *ad hoc* комитет)[6]. На основании резолюции ГА ООН A/75/282 от 2021 г. был учрежден Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, который приступил к работе в январе 2022 г.[7] и представил проект Конвенции ООН по борьбе с киберпреступностью в 2024 г.[8]

Россия и Китай, следуя повестке ООН по вопросу борьбы с киберпреступностью, всегда выступали за создание универсальной правовой базы, которая позволила бы регулировать международно-правовой режим киберпространства и режим использования информационно-коммуникационных технологий [Мозолина 2004: 152-163]. В отличие от российской и китайской позиций, США как государство, в национально-исследовательских лабораториях которого было «создано» киберпространство и Всемирная сеть, до сих пор неизменно придерживается принципа допустимости лишь минимального вмешательства государства в киберпространство и Интернет [Jackson, Davey, Sykes 1995:44-45].

Очевидно, что на начальном этапе данные противоречия не могли послужить основой для старта переговорного процесса по созданию текста Конвенции ООН по борьбе с киберпреступностью. Дискуссия по киберпроблематике продолжалась более двадцати лет и только в 2024 г. на 79-й сессии ГА ООН резолюцией 79/243 была принята Конвенция ООН против киберпреступности[9]. Означает ли это, что государствам удалось разработать и принять универсальный международный договор по кибертематике, или существует риск того, что Конвенция может рассматриваться как компромисс ради компромисса?

Правовой анализ истории подготовки данного документа представляет особый интерес. До 2024 г. не существовало единого, универсального международно-правового договора, направленного на пресечение киберпреступности. На региональном уровне, в рамках Совета Европы, действовала (и продолжает действовать) Будапештская конвенция по киберпреступности 2001 г., в которой участвуют 78 государств (что составляет 47 % от общего числа государств – членов ООН)[10]. В начале 2025 г., 10 января, к Будапештской конвенции присоединилась Руанда[11].

Поскольку с момента принятия данного договора прошло более двадцати лет, киберпреступниками были созданы новые механизмы для осуществления противоправной деятельности

---

[6] ООН: Резолюция, принятая ГА 27 декабря 2019 г. [по докладу Третьего комитета (A/74/401)] 74/247. Противодействие использованию информационнокоммуникационных технологий в преступных целях. URL: https://documents.un.org/doc/undoc/gen/n19/440/31/pdf/n1944031.pdf (дата обращения: 10.02.2025).

[7] ООН: Резолюция, принятая ГА 26 мая 2021 г. [без передачи в главные комитеты (A/75/L.87/Rev.1 и A/75/L.87/Rev.1/Add.1)] 75/282. Противодействие использованию информационно-коммуникационных технологий в преступных целях. URL: https://docs.un.org/ru/A/RES/75/282 (дата обращения: 10.02.2025).

[8] Обновленный проект текста Конвенции ООН против киберпреступности (преступлений, совершаемых с использованием информационно-коммуникационной системы). URL: https://ifap.ru/pr/2024/n240729a.pdf (дата обращения: 10.02.2025).

[9] ООН: Резолюция, принятая ГА 24 декабря 2024 г. [по докладу Третьего комитета (A/79/460, пункт 15)] 79/243. 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. URL: https://documents.un.org/doc/undoc/gen/n24/426/76/pdf/n2442676.pdf (дата обращения: 10.02.2025).

[10] Совет Европы: Будапештская конвенция 2001 г. URL: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/ (дата обращения: 10.02.2025).

[11] T-CY News: Rwanda becomes the 78th Party to the Convention on Cybercrime and accedes to the First Protocol. URL: https://www.coe.int/en/web/cybercrime/-/rwanda-becomes-the-78th-party-to-the-convention-on-cybercrime-and-accedes-to-the-first-protocol (accessed date: 10.02.2025).

на «новой территории» в международном праве. С учетом того, что в 2022 г. Россия перестала быть государством – членом Совета Европы, вопрос создания Конвенции против киберпреступности на уровне ООН для российской стороны стал еще более актуальным[12].

Разногласия на этапе разработки текста Конвенции против киберпреступности первоначально носили непримиримый характер. Один из важнейших вопросов заключался в том, какие составы преступлений могут быть отнесены к «кибернетическим»? Россия и Китай, например, исходили из того, что это могут быть *все незаконные акты, которые связаны с использованием кибертехнологий*. Подобный перечень включает в себя высказывание «противоправных» суждений и разжигание неприязни по политическим, социальным, этническим и другим мотивам в Интернете, что было отражено в Доктрине информационной безопасности Российской Федерации от 2016 г.[13]

Так, изначально наименование данного договора – Конвенция против киберпреступности (полное наименование: Конвенция 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) вызвало разногласия России и Китая с рядом других государств, прежде всего, США. Российская и китайская стороны предлагали иное наименование – Проект Конвенции ООН о противодействии использованию информационно-коммуникационных технологий в преступных целях[14].

Согласование наименования новой Конвенции можно отнести к одному из ключевых дискуссионных вопросов в подходах России и США к киберпространству в целом и к киберпреступности в частности. Как известно, ряд западных государств (Канада, Великобритания, государства – члены Европейского союза), а также США используют более широкую формулировку *«киберпространства» (cyberspace)* [Assaf 2023:4-21], который включает в себя *технологическую составляющую (т.е. сами компьютерные системы),* тогда как Россия и Китай используют такое понятие как термин «информационно-коммуникационные технологии» с возможностью ограничения использования ИКТ в преступных целях, т.е. посредством использования данного понятийного аппарата в государстве вводится возможность некоего «цензурирования» Интернета, против которого категорически выступают США и другие «западные государства» [Godwin, Kulpin, Rauscher, Yaschenko 2014:11].

В рамках переговорного процесса было выбрано одно из промежуточных наименований документа – Проект Конвенции ООН против киберпреступности; укрепление международного сотрудничества в борьбе с определенными преступлениями, совершаемыми с использованием информационно-коммуникационных технологий, и в обмене доказательствами в электронной форме, относящимися к серьезным преступлениям.

По мнению заместителя директора департамента Международной информационной безопасности (далее – МИБ) МИД России Д.В. Букина, Россия при подписании документа планирует сделать соответствующее толковательное заявление относительно наименования конвенции[15]. Несогласие с наименованием Конвенции помимо России выразили Китай и Иран, обозначив необходимость пересмотреть наименование договора. Применительно к защите пользователей Интернета данный спор государств на уровне ООН представляется отнюдь не теоретическим, а практическим, поскольку юридическое наполнение терминов «ИКТ» и «киберпространство» различно. В случае пресечения противоправной деятельности в сегменте Даркнета подобный подход российской стороны оправдан защитой интересов государства и общества в целом,

[12] МИД России: О выходе России из Совета Европы (справочный материал). URL: https://www.mid.ru/ru/foreign_policy/rso/1834254/ (дата обращения: 10.02.2025).

[13] Российская газета: Доктрина информационной безопасности. Утв. Указом Президента РФ от 5 декабря 2016 г. № 646. URL: https://rg.ru/documents/2016/12/06/doktrina-infobezobasnost-site-dok.html (дата обращения: 10.02.2025).

[14] Черненко Е. Под статью подвели не все. Россия недовольна проектом конвенции ООН по борьбе с киберпреступностью. – *Коммерсантъ*. 2024. URL: https://www.kommersant.ru/doc/6452715 (дата обращения: 10.02.2025).

[15] Черненко Е. Киберчувствительная тема. Проект конвенции ООН по борьбе с компьютерной преступностью не нравится ни России, ни ее оппонентам. – *Коммерсантъ*. 2024. URL: https://www.kommersant.ru/doc/6864552 (дата обращения: 10.02.2025).

однако в случае применения данного подхода к так называемому «белому сегменту», существует риск «цензурирования» киберпространства и привлечения пользователей к ответственности по различным основаниям.

Следует обозначить, что к 2025 г. образовались три группы государств, каждая из которых ожидает от новой Конвенции реализации поставленных государством в киберпространстве задач: 1) государства, выступающие за усиление криминализации противоправной деятельности, к которым относятся Россия и Китай; 2) «западные государства», стремящиеся связать текст нового документа с имеющимся правовым регулированием в Будапештской конвенции 2001 г.; и 3) государства, рассматривающие переговорный процесс в ООН и итоговый документ в качестве механизма преодоления цифрового неравенства и усиления технического сотрудничества (например, развивающиеся страны)[16].

3. Основные положения Конвенции ООН против киберпреступности 2024 г.

Конвенция против киберпреступности 2024 г. состоит из 68 статей и 9 глав, а также Приложения «Примечания для толкования по конкретным статьям Конвенции Организации Объединенных Наций против киберпреступности…»[17], в котором в примечании к ст. 2 Конвенции указывается, что «Государства-участники не обязаны дословно воспроизводить в своем внутреннем законодательстве те же термины, определения которых даны в ст. 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». Цели Конвенции обозначены в ст. 1 следующим образом: 1) *содействие принятию и укрепление мер, направленных на повышение эффективности и результативности предупреждения киберпреступности и борьбы с ней;* 2) *поощрение и укрепление международного сотрудничества в предупреждении и борьбе с киберпреступностью;* 3) *поощрение и поддержка технической помощи и создания потенциала для предупреждения и борьбы киберпреступностью, особенно в интересах развивающихся стран.*

Перед тем как перечислить составы деяний, содержащиеся в тексте Конвенции 2024 г., необходимо провести различие между теми преступлениями, которые «обязаны своим существованием» появлению компьютеров (так называемые cyber-dependent crimes), например, получение незаконного доступа, перехват, вмешательство в компьютерные системы и теми преступлениями, которые *«совершаются с применением компьютеров»* (так называемые cyber-enabled crimes), например, распространение детской порнографии[18].

При согласовании проекта Конвенции США и ряд других западных государств предложили ограничить перечень преступлений, т.е. сфокусироваться на преступлениях, совершаемых хакерами или иными лицами в Интернете, но не журналистами, ведущими расследование, или лицами, занимающимися общественной деятельностью, которые могут стать потенциальными жертвами (potential victims) некорректного толкования положений новой Конвенции.

По итогам данной дискуссии, в Конвенции были выделены 10 составов преступлений (первоначально Россия предлагала включить 23 состава): 1) незаконный доступ к ИКТ; 2) незаконный перехват (данных); 3) воздействие на электронные данные; 4) воздействие на информационно-коммуникационную систему (далее – ИКС); 5) неправомерное использование устройств; 6) подлог с использованием ИКС; 7) хищение и мошенничество с использованием ИКС; 8) преступления, связанные с размещением в интернете материалов со сценами сексуальных надругательств над детьми или их

[16] Bannelier K., Lostri E. So Close, So Far: UN Committee Tasked With Cybercrime Convention Hits Snooze. – *Lawfare*. 2024. URL: https://www.lawfaremedia.org/article/so-close-so-far-un-committee-tasked-with-cybercrime-convention-hits-snooze (accessed date: 10.02.2025).

[17] ООН: Резолюция, принятая Генеральной Ассамблеей 24 декабря 2024 г. [по докладу Третьего комитета (A/79/460, п. 15)] 79/243. 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. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 10.02.2025).

[18] UN News: Global Cybercrime Treaty: A delicate balance between security and human rights. URL: https://news.un.org/en/interview/2024/02/1146772 (accessed date: 10.02.2025).

сексуальной эксплуатации (т.е. детская порнография); 9) домогательство или создание доверительных отношений с целью совершения сексуального преступления в отношении ребенка; 10) распространение интимных изображений без согласия (лица).

Россия и двадцать других государств (например, упомянутые ранее Китай и Иран) при обозначении наименования новой Конвенции выступали за более широкое определение «киберпреступлений» и за включение в перечень составов преступных деяний тех, совершение которых может быть фактически «упрощено» посредством использования технологий (например, осуществление экстремистской деятельности в Интернете на условиях анонимности)[19].

При сравнении текста новой Конвенции 2024 г. с текстом Будапештской конвенции 2001 г.[20] можно констатировать, что акцент в первом источнике был сделан, прежде всего, на cyber-dependent crimes, поэтому основные составы преступлений были связаны с неправомерным использованием компьютера (перехват, неправомерный доступ, мошенничество с использованием компьютеров и т.д.). Вместе с тем в Будапештской конвенции перечислены (по остаточному принципу) и cyber-enabled crimes (например, детская порнография). Стоит отметить, что данный компромиссный вариант был использован ООН, т.е. практически все виды составов преступлений, перечисленных в Будапештской конвенции 2001 г., были перенесены в текст новой Конвенции 2024 г. кроме преступлений, связанных с нарушением авторских прав.

Некоторые государства (например, Индия) при обсуждении проекта предложили внести еще такой состав, как отправление электронных сообщений, носящих грубый и оскорбительный характер с целью причинения «раздражения» [Scher-Zagier 2024:12].

Обозначим, что несмотря на длительность переговорного процесса государств – членов ООН, длившегося более двадцати лет, скорость разработки итогового текста Конвенции поражает. За 2023–2024 гг. удалось представить полноценную версию текста проекта. На официальном сайте ООН приводятся пять основных задач документа, которые будут реализованы в ближайшем будущем: 1) борьба с растущей угрозой киберпреступности по всему миру; 2) «круглосуточное» сотрудничество государств; 3) защита интересов детей в Интернете; 4) реагирование на нарушение прав пострадавших пользователей; и 5) улучшение механизма предупреждения киберпреступности[21].

На фоне положительной оценки рядом государств – членов ООН первого универсального документа, направленного на борьбу с киберпреступностью, и его (документа) единогласным принятием на заседании ГА ООН, ряд ведущих IT-компаний, транснациональных корпораций и объединений государств сохраняют сдержанный оптимизм по данному вопросу.

По оценке компании Microsoft, Конвенция против киберпреступности 2024 г. в будущем так и не даст ответы на многие существующие вопросы. Вместо этого компания предлагает развивать уже существующие механизмы защиты. Основная проблема заключается в том, что (по мнению многих IT-гигантов) в одну конвенцию невозможно включить компьютерные преступления и преступные деяния, совершаемые с использованием компьютеров, а также эффективно реализовывать уголовное преследование лиц (то, на чем настаивали Россия и Китай)[22]. Обеспокоенность в Европейском союзе вызывает применение ст. 23, в которой предусмотрена возможность осуществления государством полномочий и процедур в случае совершения «других уголовных правонарушений с использованием информационно-коммуникационной системы»,

[19] Объединенные Нации. Цифровая библиотека: Letter dated 30 July 2021 from the Chargé d'affaires a.i. of the Permanent Mission of the Russian Federation to the United Nations addressed to the Secretary-General. URL: https://digitallibrary.un.org/record/3942230?v=pdf (accessed date: 10.02.2025).

[20] Совет Европы: Будапештская конвенция 2001 г. URL: https://www.coe.int/ru/web/impact-convention-human-rights/convention-on-cybercrime#/ (дата обращения: 10.02.2025).

[21] UN News: Making the digital and physical world safer: Why the Convention against Cybercrime matters. URL: https://news.un.org/en/story/2024/12/1158526 (accessed date: 10.02.2025).

[22] Greig J. Microsoft Joins Opposition to Current Version of UN Cybercrime Treaty. – *The Record. Recorded Future News*. 2023. URL: https://therecord.media/microsoft-opposes-draft-cybercrime-treaty (accessed date: 10.02.2025).

поскольку в тексте документа государствами не были определены примерные составы таких деяний.

Помимо абстрактных примеров, связанных с обеспокоенностью компании Microsoft и Европейского союза[23], существуют реальные риски, вызванные имплементацией положений Конвенции.

С одной стороны, данный документ позволит государствам расширить сотрудничество в сфере борьбы с киберпреступностью, если между ними не были заключены так называемые договоры о взаимной правовой помощи (далее – Mutual legal assistance treaties, MLATs), или, в случае наличия таковых, будет рассматриваться как дополнительное средство правовой помощи.

С другой стороны, первая и основная проблема – возможность установления трансграничной электронной слежки за лицами, совершившими преступление, носящее «серьезный характер». Какие составы преступлений могут быть отнесены к носящим «серьезный характер»? По смыслу понятийного аппарата ст. 2 п. "h" к «серьезному преступлению» относится такое противоправное деяние, за совершение которого предусматривается лишение свободы на максимальный срок не менее четырех лет или более строгая мера наказания; в то же время более конкретный ответ на поставленный выше вопрос будет дан на национальном уровне каждым государством, что на практике может позволить экстерриториально применять национальное уголовное законодательство[24].

Данный тезис можно попытаться опровергнуть, ссылаясь на ст. 24 Конвенции 2024 г. «Условия и гарантии»[25], в которой предусматривается, что государства на основании внутреннего (национального) законодательства обязуются неукоснительно соблюдать принцип международного права – защиты прав человека и основных свобод, не допуская возможности привлечения к ответственности невиновных лиц, однако в любом случае важно понимать не только содержание новой Конвенции, процесс корректного толкования которого займет некоторое время у государств – членов ООН, но и контекст ее применения. Так, в случае с Будапештской конвенцией 2001 г. толкование осуществляется в соответствии с текстом Европейской конвенции о защите прав человека и основных свобод 1950 г. и практикой Европейского суда по правам человека.

Для принятия дополнительных протоколов по отдельным аспектам имплементации Конвенции 2024 г. потребуется получение 60 ратификаций от государств – членов ООН. Предусматривается, что документ вступит в силу через 90 дней после получения 40 ратификаций[26].

4. Правовые лакуны принятого ООН документа: есть ли решение?

Поскольку сегодня невозможно предсказать, как будет соблюдаться исполнение положений Конвенции против киберпреступности 2024 г., то следует обратить внимание на отдельные правовые лакуны документа, которые связаны, прежде всего, с двумя аспектами: 1) вопрос, связанный с реализацией так называемого «принципа пассивной юрисдикции», и 2) вопрос, связанный с защитой персональных данных пользователей Интернета.

Э.Ш. Загир в статье "Jursdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdiction" (2024) анализирует возможность злоупотребления применением «принципа пассивной юрисдикции» [Scher-Zagier 2024:3-53].

---

[23] Human Rights Watch: EU: Member States Should Vote "NO" on UN Cybercrime Treaty. URL: https://www.hrw.org/news/2024/10/21/eu-member-states-should-vote-no-un-cybercrime-treaty (accessed date: 10.02.2025).

[24] Rodriguez K. The UN Cybercrime Convention: Analyzing the Risks to Human Rights and Global Privacy. – *Just Security.* 2024. URL: https://www.justsecurity.org/98738/cybercrime-convention-human-rights/ (accessed date: 10.02.2025).

[25] «Каждое Государство-участник обеспечивает, чтобы полномочия и процедуры, указанные в настоящей главе, устанавливались, осуществлялись и применялись в соответствии с условиями и гарантиями, предусмотренными в его внутреннем законодательстве, которые должны обеспечивать защиту прав человека в соответствии с его обязательствами по международному праву прав человека и включать в себя принцип соразмерности» (ООН: Резолюция, принятая ГА 24 декабря 2024 г. [по докладу Третьего комитета (A/79/460, п. 15)] 79/243. 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. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 10.02.2025)).

[26] Центр Глобальной ИТ-кооперации: В ООН принята Конвенция по борьбе с киберпреступностью. URL: https://cgitc.ru/media/v-oon-prinyata-konventsiya-po-borbe-s-kiberprestupnostyu/ (дата обращения: 10.02.2025).

Проблема применимости юрисдикционных принципов требует отдельного пояснения. В международном праве по итогам рассмотрения дела о судне «Лотус» Постоянной палатой международного правосудия в 1927 г. было сформулировано разрешительное правило, которое предполагает рассмотрение юрисдикционных принципов при установлении уголовной юрисдикции как неких общих рамок, общего правила, от которого государства могут отступать при условии соблюдения норм международного права[27].

В отечественной науке уголовного права были сформулированы два противоположных по юридическому наполнению термина: «принцип активной юрисдикции» и «принцип пассивной юрисдикции» [Татаринов 2019:6-10]. Первый термин («принцип активной юрисдикции») означает возможность «…государства гражданства предполагаемого преступника устанавливать уголовную юрисдикцию в отношении поведения своих граждан за рубежом»; тогда как второй термин («принцип пассивной юрисдикции») означает осуществление юрисдикции «…государством гражданства жертвы преступления, совершенного не его гражданином за рубежом» [Волеводз 2009:303-323][28].

Дж.Р. Ватсон рассматривая «принцип пассивной юрисдикции», определяет его следующим образом: *пассивная юрисдикция* – это возможность государства осуществлять уголовную юрисдикцию, основанную исключительно на гражданстве жертвы, подчеркивая при этом, что США всегда выступали с критикой «пассивной юрисдикции», ссылаясь на необходимость следования «классическим» нормам международного права [Watson 1993:2].

Первоначально юрисдикция государства распространялась только на его территорию и была связана с «принципом активной правосубъектности», поскольку деяние совершалось гражданами данного государства, а отдельно в уголовном праве выделялись преступления международного характера (например, пиратство). Постепенно в правовой науке был сформулирован принцип защиты (protective principle), на основании которого государство могло осуществлять юрисдикцию в отношении тех деяний, которые затрагивали наиболее важные интересы государства или «оказывали существенное влияние на территории государства» (has a substantial effect within a state's territory), однако данный подход получил критическую оценку в науке международного права [Lenhoff 1964:5-23].

Пассивная юрисдикция, по смыслу Конвенции 2024 г., относится к возможности государства осуществлять преследование лиц в отношении всех преступлений, совершение которых было направлено против интересов гражданина или граждан данного государства. До недавнего времени данное исключение из общего правила активно применялось в гражданском праве, т.е. в системе национального права, но не в системе международного права. Подобный подход к юрисдикции государства закреплен в ст. 22 «Юрисдикция»[29].

Несмотря на то что практика применения «принципа пассивной юрисдикции» – относительно новое явление в международном праве, некоторые юристы-международники утверждают, что она может стать международным обычаем при условии соответствия субъективному и объективному элементам, предусмотренным ст. 38 Статута Международного суда ООН [Scher-Zagier 2024:32].

Комиссией международного права ООН в докладе 2006 г. уже была признана возможность существования подобной юрисдикции государства (passive personality jurisdiction). American Law Institute's Restatement также признает данную практику частью международного права, применение которой вместе с тем должно быть ограничено исключительно совершением особо тяжких преступлений, например, терроризма [Scher-Zagier 2024:22].

---

[27] Affaire du "Lotus". – *Recueil des arrêts.* Série A. N° 70. Le 7 septembre 1927. URL: https://www.icj- cij.org/public/files/permanent-court-of-international-justice/serie_A/A_10/30_Lotus_Arret.pdf (accessed date: 10.02.2025).

[28] Автор использует два термина: «принцип активной юрисдикции» ("active jurisdiction principle") и «принцип пассивной юрисдикции» ("passive (personality) jurisdiction principle").

[29] ООН: Резолюция, принятая ГА 24 декабря 2024 г. [по докладу Третьего комитета (A/79/460, п. 15)] 79/243. 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. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 10.02.2025).

Правоприменительная практика США сегодня отличается от подхода, изложенного Дж. Р. Ватсоном в 1993 г.: США отказались от возражений против «принципа пассивной юрисдикции» в отношении террористических преступлений, но не от возражений в отношении в других видов преступлений (за применение данной концепции выступает также К. Галлант [Gallant 2022:441-460]). Европейским государством, признавшим возможность использования «пассивной юрисдикции», является Франция. С 1975 г. в национальное уголовное законодательство государства было включено положение о возможности осуществления юрисдикции в отношении любого преступления, совершенного против граждан государства [Blakesley 1987:938].

При обсуждении проекта Конвенции Китай выступил с инициативой рассматривать возможность государства осуществлять юрисдикцию, руководствуясь принципом места возникновения последствий преступного деяния. Египет при обсуждении проекта Конвенции предложил использовать термин «*транснациональные преступления*», в отношении которых у государства есть право на осуществление юрисдикции, т.е. такие деяния, которые влекут за собой серьезные последствия в другой стране. В рамках переговорного процесса в ООН Индия предложила использовать юрисдикцию, основанную на местонахождении данных, а не классический территориальный подход, что было обусловлено необходимостью установления контроля над данными граждан ввиду невозможности получить доступ к трансграничным данным на основе MLATs[30].

Россия выступила за возможность осуществления пассивной юрисдикции в случае совершения преступлений в отношении юридических лиц, учрежденных или имеющих постоянное представительство на территории Российской Федерации, а также в отношении государств и правительственных органов. Если попытаться пояснить подобную аморфную формулировку, то можно сформулировать общий подход: осуществление пассивной юрисдикции в отношении любых предполагаемых преступников или выдача всех лиц, в отношении которых может быть осуществлена юрисдикция[31].

Признавая неоднозначность указанного выше подхода, в юридической практике уже были рассмотрены дела, основанные на «принципе пассивной юрисдикции». В США, например, активно обсуждалось дело Каттинга (Cutting Case), датируемое XIX в. Краткое изложение сути дела состоит в следующем: А.К. Каттинг (гражданин США) подготовил материал в техасской газете El Paso, содержащий нелестные отзывы о мексиканском издателе Э. Медина. В дальнейшем мексиканское правительство заявило о своем праве на осуществление юрисдикции в отношении всех преступлений, совершаемых против интересов мексиканцев, и, по возвращении журналиста в Мексику, ему были предъявлены обвинения в клевете. Гражданин США был первоначально приговорен к тюремному заключению, однако затем освобожден в связи с отзывом Э. Медина заявления. [Moore 1887:125]. .

Примером продолжения практики, основанной на Cutting Case, является арест в 2021 г. в Пакистане журналистов по обвинению в совершении киберпреступлений, хотя их действия затрагивали только некоторые политические комментарии в Интернете[32].

С учетом расширительного толкования уголовной юрисдикции и международного права в целом в отсутствие четких гарантий и критериев соблюдения норм права, существует риск преследования со стороны государства иностранных журналистов, общественных деятелей, которые могут привлекаться по «киберстатьям», изложенным в Конвенции против киберпреступности 2024 г.

На основе анализа Electronic Frontier Foundation, ст. 6 «Соблюдение прав человека» на практике предоставит государствам свободу действий в принятии решений о гарантиях

[30] Mahadik K. Should India vote to adopt the UN cybercrime treaty? Tech policy expert weighs in. – *The Indian Express*. 2024. URL: https://indianexpress.com/article/technology/tech-news-technology/should-india-vote-to-adopt-un-cybercrime-treaty-9527899/ (accessed date: 10.02.2025).

[31] 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. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_01.09.2023_PM.pdf (accessed date: 10.02.2025).

[32] Committee to protect Journalists: Pakistan authorities detain, investigate journalists Amir Mir and Imran Shafqat. URL: https://cpj.org/2021/08/pakistan-authorities-detain-investigate-journalists-amir-mir-and-imran-shafqat/ (accessed date: 10.02.2025).

соблюдения прав человека. Третьи государства могут активно включаться в сотрудничество при осуществлении расследований по киберпреступлениям и проводить таковые совместно с запрашивающим государством за пределами территории запрашивающего государства, однако в таком случае возникают коллизионные вопросы и проблема конкурирующей юрисдикции[33].

В практике современных международных договоров, посвященных преступлениям международного характера, уже предусмотрено ограничение пассивной юрисдикции. Например, в ст. 2 Конвенции ООН о борьбе против незаконного оборота наркотических и психотропных веществ 1988 г. содержится следующий принцип: «Сторона не осуществляет на территории другой Стороны юрисдикции и функций, которые входят исключительно в компетенцию органов этой другой Стороны в соответствии с ее национальным законодательством»[34].

Более того, если обратиться тексту Будапештской конвенции 2001 г. или Таллинского руководства в редакции 2017 г. [Schmitt 2017:51-78], то применение пассивной юрисдикции оценивается как возможное только в определенных случаях (например, в случае совершения террористического акта).

Другим, не менее важным вопросом является экстрадиция лиц, совершивших преступления. Как будет регулироваться данный вопрос, если по некоторым составам выдача по национальному законодательству невозможна (например, политические преступления, военные, налоговые)?

В новой Конвенции подобные положения (а именно по налоговым преступлениям) были одобрены *ad referendum* (т.е. с возможностью последующего одобрения государством). За включение политических преступлений в перечень тех деяний, которые могут повлечь за собой выдачу лица, выступали Россия, Пакистан и Уругвай[35]. Можно привести еще один пример – п. 2 ст. 6 Конвенции, против включения которой выступал Иран. В ней речь идет о возможном отказе в международных запросах на предоставление персональных данных в том случае, если существует риск преследования по политическим взглядам, на основании расовой, этнической принадлежности и т.д.[36]

Помимо применения «принципа пассивной юрисдикции», в Конвенции 2024 г. ряд государств (прежде всего, государств – членов Европейского союза) выступили с критикой статей, посвященных защите персональных данных пользователей и дальнейшей возможности передачи данных о потенциальных киберпреступниках. Правовая позиция европейских государств заключается в том, что данный источник не посвящен проблеме борьбы с киберпреступностью как таковой[37]. Вместо этого целью государств было установление электронной слежки за конечными пользователями и наказание лиц по составам, которые не предполагают напрямую использование ИКТ. Упомянутая ранее ст. 23 также относится к вопросу защиты данных, с одной стороны, и к получению доказательств, с другой стороны: «За исключением случаев, когда в настоящей Конвенции предусмотрено иное,

---

[33] Electronic Frontier Foundation: The UN General Assembly and the Fight against the Cybercrime Treaty. URL: https://www.eff.org/deeplinks/2024/08/un-general-assembly-and-fight-against-cybercrime-treaty (accessed date: 10.02.2025).

[34] ООН: Конвенция ООН о борьбе против незаконного оборота наркотических и психотропных веществ 1988 г. URL: https://www.unodc.org/pdf/convention_1988_ru.pdf (дата обращения: 10.02.2025).

[35] Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes Fifth session Vienna, 11–21 April 2023 Consolidated negotiating document on the preamble, the provisions on international cooperation, preventive measures, technical assistance and the mechanism of implementation and the final provisions of a comprehensive international convention on countering the use of information and communications technologies for criminal purposes. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf (accessed date: 10.02.2025).

36 «Ничто в настоящей Конвенции не толкуется как допускающее подавление прав человека или основных свобод, включая права, касающиеся свободы выражения, совести, мнений, религии или убеждений, мирных собраний и объединений, в соответствии с применимыми нормами международного права прав человека» (ООН: Резолюция, принятая ГА 24 декабря 2024 г. [по докладу Третьего комитета (A/79/460, п. 15)] 79/243. 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. URL: https://docs.un.org/ru/A/RES/79/243 (дата обращения: 10.02.2025)).

[37] Hassan T. Upcoming Cybercrime Treaty will be Nothing but Trouble. – *Human Rights Watch*. 2024. URL: https://www.hrw.org/news/2024/08/07/upcoming-cybercrime-treaty-will-be-nothing-trouble (accessed date: 10.02.2025).

каждое Государство-участник применяет полномочия и процедуры, указанные в пункте 1 настоящей статьи, в отношении: a) уголовных правонарушений, признанных таковыми в соответствии с настоящей Конвенцией; b) других уголовных правонарушений, совершенных с помощью информационно-коммуникационной системы; и c) сбора доказательств в электронной форме, относящихся к любому уголовному правонарушению». Предложение некоторых общественных организаций, занимающихся вопросами защиты прав человека, заключалось в том, чтобы внести в п. "b" и "c" указание на возможность получения данных только в случае наличия серьезных оснований полагать, что преступление носит «серьезный характер»[38]. Безусловно, передать данные можно будет в случае совершения именно подобной категории преступлений («серьезных» согласно терминологии Конвенции), т.е. срок наказания по которым по внутреннему законодательству составляет от четырех лет и выше, однако в дальнейшем (например, при разработке дополнительных протоколов) было бы целесообразно повысить уровень гарантий для лиц, осуществляющих свою деятельность в Интернете (блогеры, журналисты, общественные деятели).

5. Заключение

Подводя итог изложенному выше, следует попытаться оценить итоги «кибернормотворчества» государств – членов ООН.

С одной стороны, на универсальном уровне был впервые подготовлен и принят документ, который направлен на борьбу с киберпреступностью. С другой стороны, ведущее значение государства в киберпространстве постепенно утрачивается, тогда как роль не субъектов международного права (в частности, IT-гигантов и занимающих их сторону общественных организаций) увеличивается. Следовательно, возможно следовать общемировым тенденциям по борьбе с киберпреступностью и, в частности, тем мерам, которые предпринимаются крупнейшими компаниями, занимающимися киберпроблематикой.

Если позиция США и ряда других западных государств изначально заключалась в отрицании возможности представить в ООН для рассмотрения подобный документ, то сейчас фокус внимания данных государств сместился в сторону использования Конвенции против киберпреступности 2024 г. в целях защиты, прежде всего, государственных интересов. К. Баннелье и Е. Лостри отмечают, что включение в переговорный процесс США и Великобритании было обусловлено желанием «не остаться в стороне» и сосредоточить внутригосударственные усилия на стадии «наиболее выгодного толкования» данного источника международного права[39]. Ряд американских представителей заявили, что «договор лишь позволит увеличить число государств, которые будут реагировать на американские ордера на арест, связанные с киберпреступлениями[40].

Возможно, что с учетом того правового хаоса, который связан с освоением киберпространства, выражающегося, например: 1) в невозможности согласовать единый подход к терминологическому аппарату; 2) отсутствии единства в возможности «цензурирования» Интернета; 3) смещении фокуса внимания с киберпространства в сторону искусственного интеллекта и нейроправ [Ситников 2024:69-93], Конвенция ООН против киберпреступности 2024 г. может стать еще одним камнем преткновения в позициях государств, а не итогом заявленного компромисса.

Список литературы

1. Волеводз А.Г. 2009. Современная система международной уголовной юстиции: понятие, правовые основы, структура и признаки. – *Международное уголовное правосудие: Современные проблемы.* Москва: Институт права и публичной политики. С. 303-323.
2. Данельян А.А. 2020. Международно-правовое регулирование киберпространства. – *Образование и право.* № 1. С. 261-269.
3. Иноземцев М.И. 2021. Цифровое право: в поисках определенности. – *Digital Law Journal.* Vol. 2. № 1. С. 18-28.
4. Комова Е.Ю., Сидоренко Э.Л. Использование цифровых технологий на фондовом рынке: уголовно-правовой аспект. – *Digital Law Journal.* Vol. 4. № 1. С. 74-85.
5. Мозолина О.В. 2004. Вопросы международно-правового регулирования Интернета. – *Московский журнал международного права.* № 4. С. 152-163.

[38] Hassan T. Op. cit..

[39] Bannelier E., Lostri E. Is Anyone Happy With the UN Cybercrime Convention? – *Lawfare*. 2024. URL: https://www.lawfaremedia.org/article/is-anyone-happy-with-the-un-cybercrime-convention (accessed date: 10.02.2025).

[40] Greig J. Controversial UN Cybercrime Treaty Clears Final Hurdle Before Full Vote as US defends Support. – *The Record. Recorded Future News.* 2024. URL: https://therecord.media/un-cybercrime-treaty-clears-vote (accessed date: 10.02.2025).

6. Ситников М.С. 2024. Как и зачем регулировать сферу метавселенных? – *Digital Law Journal*. Vol. 5. № 1. С. 69-93.
7. Татаринов М.К. 2019. Традиционные и новые подходы к понятию и классификации юрисдикции. – *Международное публичное и частное право*. № 1. С. 6-10.
8. Assaf A. 2023. Violations of Sovereignty in "Cyberspace" under the United Nations Charter. – *Журнал ВШЭ по международному праву*. Vol. 1. № 3. С. 4-20.
9. Blakesley C.L. 1987. Jurisdiction as Legal Protection Against Terrorism. – *Connecticut Law Review*. Vol. 19. P. 895-943.
10. Clarke R.A., Knake R.K. 2019. T*he Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Publ. Penguin Press. 352 p.
11. Gallant K.S. 2022. *International Criminal Jurisdiction. Whose Law Must We Obey?* Oxford University Press. 808 p.
12. Godwin III J.B., Kulpin A., Rauscher K.F., Yaschenko V. 2014. *Critical Terminology Foundations 2. Russia. U.S. Bilateral on Cybersecurity*. Policy report. 82 p.
13. Jackson J.H., Davey W.J., Sykes A.O. 2008. *Legal Problems of International Economic Relations*. 1st ed. West Academic Publishing. 1304 p.
14. Khanna P. 2018. State Sovereignty and Self-Defence in Cyberspace. – *BRICS Law Journal*. № 5 (4). P. 139-154.
15. Lenhoff A. International Law and Rules on International Jurisdiction. - *Cornell Law Quarterly*. 1964. Vol.50. P.5-23.
16. Moore J.B. 1887. *Report on Extraterritorial Crime and the Cutting Case*. Washington DC. Government Printing Office. 130 p.
17. Scher-Zagier E. 2024. Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdition. – *Yale Journal of Law& Technology*. Vol. 27. 53 p.
18. Schmitt M.N. 2017. *Tallin Manual 2.0. On the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press. 598 p.
19. Shaw M.N. 2021. *International Law*. 9th ed. Cambridge University Press. 1213 p.
20. Watson G.R. The Passive Personality Principle. - *Texas International Law Journal*. Vol.28:1. P.1-46.

References

1. Assaf A. Violations of Sovereignty in "Cyberspace" under the United Nations Charter. – *Zhurnal VSHE po mezhdunarodnomu pravu [The HSE Journal of International Law]*. 2023. Vol. 1. № 3. P. 4-20.
2. Blakesley C.L. Jurisdiction as Legal Protection Against Terrorism. – *Connecticut Law Review*. 1987. Vol. 19. P. 895-943.
3. Clarke R.A., Knake R.K. *The Fifth Domain: Defending Our Country, Our Companies, and Ourselves in the Age of Cyber Threats*. Publ. Penguin Press. 2019. 352 p.
4. Danelyan A.A. Mezhdunarodno-pravovoe regulirovanie kiberprostranstva [International Legal Regulation of Cyberspace]. – *Obrazovanie i pravo [Education and Law]*. 2020. № 1. P. 261-269. (In Russ.).
5. Gallant K.S. *International Criminal Jurisdiction. Whose Law Must We Obey?* Oxford University Press. 2022. 808 p.
6. Godwin III J.B., Kulpin A., Rauscher K.F., Yaschenko V. *Critical Terminology Foundations 2. Russia. U.S. Bilateral on Cybersecurity*. Policy report. 2014. 82 p.
7. Inozemtsev M.I. Cifrovoe pravo: v poiskah opredelennosti [Digital Law: The Pursuit of Certainty]. – *Digital Law Journal*. 2021. Vol. 2. №1. P. 18-28. (In Russ.).
8. Jackson J.H., Davey W.J., Sykes A.O. *Legal Problems of International Economic Relations*. 1st ed. West Academic Publishing. 2008. 1304 p.
9. Khanna P. State Sovereignty and Self-Defence in Cyberspace. – *BRICS Law Journal*. 2018. № 5(4). P. 139-154.
10. Komova E. Yu., Sidorenko E.L. Ispol'zovanie cifrovyh tehnologij na fondovom rynke: ugolovno-pravovoj aspect [Using Digital Technologies in the Stock Market: the Criminal Law Aspect]. – *Digital Law Journal*. Vol. 4. № 1. P. 74-85. (In Russ.).
11. Lenhoff A. International Law and Rules on International Jurisdiction. - *Cornell Law Quarterly*. 1964. Vol. 50. P. 5-23.
12. Moore J.B. *Report on Extraterritorial Crime and the Cutting Case*. Washington DC. Government Printing Office. 1887. 130 p.
13. Mozolina O.V. Voprosy mezhdunarodno-pravovogo regulirovanija Interneta[Issues of international Legal Regulation of the Internet]. – *Moskovskij zhurnal mezhdunarodnogo prava [Moscow Journal of International Law]*. 2004. № 4. P. 152-163. (In Russ.).
14. Scher-Zagier E. Jurisdictional Creep: The UN Cybercrime Convention and the Expansion of Passive Personality Jurisdition. – *Yale Journal of Law& Technology*. 2024. Vol. 27. 53 p.
15. Schmitt M.N. *Tallin Manual 2.0. On the International Law Applicable to Cyber Operations*. 2nd ed. Cambridge University Press. 2017. 598 p.
16. Shaw M.N. *International Law*. 9th ed. Cambridge University Press. 2021. 1213 p.
17. Sitnikov M.S. Kak i zachem regulirovat' sferu metavselennyh? [How and why should we regulate the metaverse?]. – *Digital Law Journal*. 2024. Vol. 5. № 1. P. 69-93. (In Russ.).
18. Tatarinov M.K. Tradicionnye i novye podhody k ponjatiju i klassifikacii jurisdikcii [Traditional and New Approaches to the Concept and Classification of Jurisdiction]. – *Mezhdunarodnoe publichnoe i chastnoe pravo [International Public and Private Law]*. 2019. № 1. P. 6-10. (In Russ.).
19. Volevodz A.G. Sovremennaja sistema mezhdunarodnoj ugolovnoj justicii: ponjatie, pravovye osnovy, struktura i priznaki [Modern system of international criminal justice system: legal basis, structure and features]. – *Mezhdunarodnoe ugolovnoe pravosudie: Sovremennye problem [International Criminal Justice: Modern Problems]*. Moscow: Institut prava i publichnoj politiki. 2009. P. 303-323. (In Russ.).
20. Watson G.R. The Passive Personality Principle. - *Texas International Law Journal*. 1993. Vol.28:1. P.1-46.

Информация об авторе

Дарья Дмитриевна ШТОДИНА,
кандидат юридических наук, научный сотрудник Департамента Международного права ВШЭ, Национальный исследовательский университет «Высшая школа экономики»

Большой Трехсвятительский пер., д. 3, Москва, 109028, Российская Федерация

dashashtodina96@gmail.com
ORCID: 0000-0003-4730-9614

About the Author

Daria D. SHTODINA,
Candidate of Legal Sciences, Research Associate, Department of International Law, National Research University Higher School of Economics

3, Bolshoy Tryokhsvyatitelsky Ln., Moscow, Russian Federation, 109028

dashashtodina96@gmail.com,
ORCID: 0000-0003-4730-9614