LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 3(2026) / ISSN 3030-3052 Available at www.uznauka.uz

# НОВЫЙ ДОГОВОР ООН ПО КИБЕРПРЕСТУПНОСТИ: ПРАВОВЫЕ ВЫЗОВЫ УНИВЕРСАЛИЗАЦИИ МЕЖДУНАРОДНЫХ СТАНДАРТОВ

**Атаханов Ш.**
Независимый соискатель

***Аннотация.*** *в статье анализируется процесс разработки и принятия нового универсального договора Организации Объединённых Наций по борьбе с киберпреступностью, его соотношение с существующими региональными инструментами и возникающие правовые вызовы в контексте универсализации международных стандартов. Особое внимание уделяется проблемам коллизионности норм, различиям в правовых системах государств, вопросам соблюдения прав человека и обеспечению процессуальных гарантий. Делается вывод о том, что универсализация возможна лишь при условии соблюдения баланса между эффективностью уголовного преследования и защитой фундаментальных прав и свобод.*

***Ключевые слова:*** *киберпреступность, универсальный договор, ООН, международное уголовное право, права человека, цифровой суверенитет, гармонизация законодательства.*

Новый договор Организации Объединённых Наций по киберпреступности стал одним из наиболее значимых международно-правовых проектов последних лет в сфере регулирования цифрового пространства. Его появление обусловлено стремительным ростом трансграничной киберпреступности, развитием технологий искусственного интеллекта, цифровых финансовых инструментов и облачных сервисов, а также объективной необходимостью формирования универсального механизма сотрудничества государств [1]. Если ранее международное

регулирование носило преимущественно региональный характер, то современный этап характеризуется попыткой выработки глобального нормативного стандарта, применимого ко всем государствам вне зависимости от их правовой системы и уровня технологического развития [2].

До начала переговоров по универсальному договору ключевым международным инструментом оставалась Конвенция о киберпреступности, принятая в 2001 году в Будапеште в рамках Совета Европы. Указанная Конвенция закрепила основные составы киберпреступлений, включая незаконный доступ к компьютерным системам, вмешательство в данные и системы, компьютерное мошенничество и преступления, связанные с детской порнографией, а также установила процессуальные механизмы сохранения и изъятия электронных доказательств. Впоследствии к ней был принят Второй дополнительный протокол о расширенном сотрудничестве и раскрытии электронных доказательств [3]. Несмотря на открытый характер документа и присоединение к нему ряда государств за пределами Европы, многие страны критиковали его как продукт регионального формата, разработанный без их полноценного участия, что, по их мнению, ограничивало его универсальную легитимность [4].

В 2019 году Генеральная Ассамблея Организация Объединённых Наций приняла резолюцию о создании специального межправительственного комитета для разработки всеобъемлющей международной конвенции по борьбе с использованием информационно-коммуникационных технологий в преступных целях [5]. Переговорный процесс, продолжавшийся несколько лет, завершился согласованием текста нового универсального договора. Его

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 3(2026) / ISSN 3030-3052 Available at www.uznauka.uz

цель заключается в укреплении международного сотрудничества, унификации уголовно-правовых подходов и создании процедурных механизмов, позволяющих эффективно расследовать преступления в киберпространстве [6].

Одним из ключевых правовых вызовов универсализации международных стандартов стала необходимость согласования различных правовых систем. Государства, принадлежащие к романо-германской, англосаксонской, смешанной и религиозно-правовой традиции, по-разному определяют элементы состава преступления, стандарты доказывания, допустимость электронных доказательств и пределы уголовной ответственности [7]. Универсальный договор неизбежно носит компромиссный характер, поскольку его положения должны учитывать разнообразие национальных моделей уголовного процесса. В результате многие формулировки имеют рамочный характер, что обеспечивает гибкость имплементации, но одновременно создаёт риск неоднородного толкования и применения норм [8].

Существенные разногласия возникли по вопросу объёма криминализации. В ходе переговоров обсуждалось, должны ли в договор включаться только так называемые «ядровые» киберпреступления либо также преступления, связанные с распространением запрещённой информации, экстремистских материалов или вмешательством в информационный суверенитет государства [9]. Расширительное толкование перечня преступлений вызвало обеспокоенность со стороны государств и международных правозащитных организаций, поскольку такие положения потенциально могут затрагивать свободу выражения мнения,

LAW, POLICY AND SOCIETY ПРАВО, ПОЛИТИКА И ОБЩЕСТВО - HUQUQ, SIYOSAT VA JAMIYAT
ILMIY-TAHLILIY JURNAL
Issue - 3(2026) / ISSN 3030-3052 Available at www.uznauka.uz

гарантированную, в частности, Международным пактом о гражданских и политических правах 1966 года. Таким образом, универсализация стандартов оказалась тесно связанной с необходимостью соблюдения международных обязательств в области прав человека [10].

Не менее важной стала проблема обеспечения процессуальных гарантий. Эффективное расследование киберпреступлений требует оперативного сохранения данных, перехвата трафика, доступа к облачным хранилищам и трансграничного обмена информацией. Однако такие меры неизбежно затрагивают право на неприкосновенность частной жизни и защиту персональных данных. В этой связи в тексте договора подчёркивается необходимость соблюдения принципов законности, необходимости и пропорциональности вмешательства[11]. Вопрос о трансграничном доступе к данным стал одним из наиболее дискуссионных, поскольку он непосредственно затрагивает принцип государственного суверенитета и запрет вмешательства во внутренние дела.

Особого внимания заслуживает соотношение нового универсального договора с Конвенция о киберпреступности. Существование двух параллельных международно-правовых режимов может привести к фрагментации регулирования, различиям в стандартах и конкуренции процедур. Вместе с тем универсальный договор имеет потенциал стать более инклюзивной платформой сотрудничества, объединяющей государства, которые ранее не участвовали в региональных инициативах. В долгосрочной перспективе возможно формирование взаимодополняющей модели, при которой универсальные стандарты будут служить минимальной основой, а

Issue - 3(2026) / ISSN 3030-3052 Available at www.uznauka.uz

региональные инструменты — обеспечивать более высокий уровень детализации [12].

Таким образом, новый договор Организации Объединённых Наций по киберпреступности отражает стремление международного сообщества создать универсальный правовой механизм противодействия преступлениям в цифровой среде. Однако процесс универсализации международных стандартов сопровождается серьёзными вызовами, связанными с различиями правовых систем, балансом между безопасностью и правами человека, вопросами цифрового суверенитета и риском нормативной фрагментации. Эффективность данного договора в значительной степени будет зависеть от добросовестной имплементации его положений на национальном уровне, от сохранения высокого уровня правовых гарантий и от способности государств выстроить доверительное и устойчивое сотрудничество в условиях быстро меняющейся цифровой реальности.

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ:

1. Лазаренкова, И. Ю. (2025). Международно-правовые механизмы противодействия транснациональной киберпреступности: вызовы унификации и проблемы имплементации в национальные правовые системы. *Вопросы российского и международного права*, *15*(2-1), 69-83.

2. Кикоть-Глуходедова, Т. В. (2025). Кибербезопасность и права человека в цифровых средах: международно-правовые вызовы и перспективы. *Закон и право*, (10), 90-97.

Issue - 3(2026) / ISSN 3030-3052 Available at www.uznauka.uz

3. Нешатаева, Т. Н. МЕЖДУНАРОДНО-ПРАВОВОЕ РЕГУЛИРОВАНИЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПЛЕНИЯМ.

4. Абделькарим, Я. А. (2025). Конвенция Организации Объединенных Наций против киберпреступности: имплементация концепции взаимной правовой помощи в цифровую эпоху. *Journal of Digital Technologies and Law*, *3*(4), 543-569.

5. ЕЖЕГОДНОЙ, М. Х., & БЛИЩЕНКО, П. (2012). Актуальные проблемы современного международного права. *Материалы*, *13*, 14.

6. Козаев, Н. Ш. (2024). Киберпреступность в современном мире: тенденции, вызовы и стратегии противодействия. *Гуманитарные, социально-экономические и общественные науки*, (11), 146-153.

7. Ефимова, А. И. (2010). Развитие международного сотрудничества по противодействию организованной преступности: ценностный выбор мирового сообщества. *Вестник МГИМО Университета*, (3), 172-178.

8. Бекяшев, К. А. (2015). Сможет ли глобализация изменить международное право?. *Вестник университета имени ОЕ Кутафина*, (6), 38-53.

9. Буз, С. И. (2019). Киберпреступления: понятие, сущность и общая характеристика. *Юристъ-правоведъ*, (4 (91)), 78-82.

10. Бородкина, Т. Н., & Павлюк, А. В. (2018). Киберпреступления: понятие, содержание и меры противодействия. *Социально-политические науки*, (1), 135-137.

11. Витвицкая, С. С., Витвицкий, А. А., & Исакова, Ю. И. (2023). Киберпреступления: понятие, классификация, международное противодействие. *Правовой порядок и правовые ценности*, *1*(1), 126-136.

12. Косолапов, Ю. В., Костромина, Е. А., & Сивова, А. А. (2018). Киберпреступления в индустрии финансовых услуг. *Вопросы экономики и права*, (118), 25-29.