Отчет о деятельности ООН: События, связанные с киберпространством

Отчет для ООН: События, связанные с киберпространством, в рамках Рабочей группы открытого состава по безопасности и использованию информационно-коммуникационных технологий (РГОС), Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (АНС), Глобального цифрового договора (GDC) и других дискуссий, связанных с ООН.

GE-014
15 декабря 2023 года

ICANN

СОДЕРЖАНИЕ

Введение

В документе представлен отчет о деятельности Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН), связанной с обсуждением вопросов киберпространства. Он включает в себя обновленную информацию, полученную в ходе обсуждений в рамках второй Рабочей группы открытого состава (РГОС)[1] и Специального комитета экспертов (СКЭ)[2] в период с 4 июня 2021 года по 2 сентября 2023 года, а также последние обсуждения Глобального цифрового договора в 2023 году и связанных с ним вопросов.

В этом документе, являющемся одним из периодических отчетов, представлен обзор мероприятий, проводимых в ООН, которые имеют отношение к экосистеме Интернета и миссии Интернет-корпорации по присвоению имен и номеров.[3] Мониторинг такой деятельности демонстрирует готовность и обязанность отдела по взаимодействию с правительствами и межправительственными организациями (GE) корпорации ICANN информировать все сообщество о вопросах, представляющих важность для глобального единого функционально совместимого интернета и его системы уникальных идентификаторов.[4]

[1] Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий (РГОС), https://meetings.unoda.org/meeting/57871/statements
[2] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home
[3] Предыдущие отчеты GE см. здесь: https://www.icann.org/en/government-engagement/publications Этот и все остальные URL в сносках и приложениях были загружены [вставить] августа 2023 года.
[4] «План операционной деятельности и финансовый план ICANN», стр. 47, корпорация ICANN, декабрь 2020 года, https://www.icann.org/en/system/files/files/draft-op-financial-plan-fy21-25-opplan-fy21-20dec19-en.pdf

Отчет РГОС

Первая основная сессия[5]

9 декабря 2021 года

Китай: «Существующая система распределения и управления важнейшими интернет-ресурсами несбалансирована и несправедлива». [...] «Государства должны участвовать в управлении и распределении международных интернет-ресурсов на равных условиях и создать глобальную систему управления интернетом, основанную на принципах многосторонности, демократии и транспарентности».[6]

12 декабря 2021 года

Китай: «Государства имеют право осуществлять, в соответствии с общепризнанными принципами и нормами международного права, необходимую и разумную личную, территориальную и защитную юрисдикцию в отношении конкретных видов деятельности в сфере ИКТ за пределами их территорий, которые имеют реальную и существенную связь с государствами, а также в отношении соответствующих объектов, организаций, данных и информации, связанных с ИКТ. Для осуществления своей юрисдикции государство может обращаться за помощью к другим государствам и регионам в духе сдержанности, вежливости и взаимности».
[...]
«Проявление суверенитета на физическом уровне. Государства обладают юрисдикцией в отношении физической инфраструктуры и базовых услуг ИКТ на своей территории. Государства имеют право принимать необходимые меры для поддержания безопасности физической инфраструктуры согласно национальному законодательству и в соответствии с международным правом. Государства имеют право участвовать в управлении и международном сотрудничестве в области глобальной инфраструктуры Интернета». [...] «Проявление суверенитета на логическом уровне. Государства могут самостоятельно вводить в действие или принимать соответствующие технические правила или стандарты, сохраняя при этом функциональную совместимость Интернета в соответствии со своими обязательствами по международному праву».[7]

Контекст. В недавнем документе, выпущенном Информационным управлением Государственного совета Китайской Народной Республики, приводятся следующие положения, касающиеся управления и критических интернет-ресурсов:

«Глава III, пункт № 3: Активное участие в управлении киберпространством
Китай активно участвует в работе глобальных интернет-организаций. Он активно участвует в деятельности таких платформ и организаций, как Интернет-корпорация

[5] Цитаты с заседаний РГОС и АНС включают как письменные, так и устные заявления
[6] Мнение Китая о применении принципа суверенитета в киберпространстве, 9 декабря 2021 г., стр. 1, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-International-Rules-making-in-Cyberspace-ENG.pdf
[7] Мнение Китая о применении принципа суверенитета в киберпространстве, 12 декабря 2021 г., стр. 1 и 4, https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf

по присвоению имен и номеров (ICANN). Он поддержал реформу механизма управления ICANN, чтобы увеличить представительство развивающихся стран и передать больше информационных ресурсов интернета под согласованное глобальное управление. Китай также участвует в деятельности Общества Интернета (ISOC), Инженерной проектной группы интернета (IETF) и Совета по архитектуре Интернета (IAB). Он играет конструктивную роль в содействии обмену между сообществами, продвижении технических исследований и разработок и их применении, а также принимает активное участие в разработке соответствующих стандартов и правил».
[...]

«Глава IV, пункт № 5: 5. Поддержание безопасности и стабильности системы управления основными ресурсами Интернета
Система управления основными ресурсами интернета — это краеугольный камень интернет-операций. Необходимо гарантировать, что учреждения, размещающие у себя системы управления, работают с полным доверием и не представляют угрозы для доменов верхнего уровня какой-либо страны только из-за юрисдикционных требований к другой стране. Китай выступает за гарантированную доступность и надежность основных интернет-ресурсов, которые будут использоваться всеми странами, совместно управляться и справедливо распределяться международным сообществом, чтобы технологические системы для этих ресурсов, включая систему доменных имен, были безопасными, стабильными и устойчивыми. Должна быть гарантия того, что услуги не будут прерваны или прекращены из-за каких-либо политических или человеческих факторов. Китай выступает за то, чтобы правительства, отраслевые регулирующие органы и предприятия совместно работали над ускорением использования технологий и приложений IPv6».[8]

[8] Синьхуа, «Китай публикует документ о сообществе с единым будущим в киберпространстве», 7 ноября 2022 г. https://english.www.gov.cn/archive/whitepaper/202211/07/content_WS636894aac6d0a757729e2973.html

14 декабря 2021 года

Португалия: «Мощные совместные международные усилия по обеспечению устойчивости национальных критических инфраструктур всех стран-членов ООН и связывающего их интернет-ядра, осуществляемые в соответствии с правами человека, международным правом и высочайшими стандартами, необходимы для сдерживания кибератак ниже порога вооруженного конфликта».[9]

Китай: «Будущее интернета не должно и не может контролироваться горсткой стран. Формирование идеологически эксклюзивных малых кругов, цепляющихся за монополию ИКТ и кибернетическую гармонию, будет только мешать многосторонним усилиям по продвижению кибербезопасности. Некоторые страны попытались создать так называемый «Альянс за будущее интернета», который является ничем иным, как примером попыток разделить интернет, добиться технологической монополии и гегемонии в киберпространстве и подавить научно-техническое развитие других стран только для того, чтобы обслуживать собственные геополитические цели. Они заявляют, что хотят создать открытый интернет, но на самом деле разжигают конфронтацию и разделяют интернет, что полностью противоречит духу мира, безопасности, открытости и сотрудничества, а также общим интересам международного сообщества».[10]

«Тем временем мы должны, в соответствии с атрибутами ИКТ и потребностями развивающейся ситуации, обсудить формулирование новых норм. Безопасность данных — новая серьезная проблема, с которой сталкиваются все страны. В соответствии с мандатом резолюции стороны проведут углубленное обсуждение вопросов трансграничного обмена данными, безопасности цепочек поставок и защиты личной информации, а также изучат соответствующие ответные меры. Китайская глобальная инициатива по безопасности данных может послужить предварительной основой для обсуждения».[11]

Контекст. IB этом же заявлении содержится критика инициатив других стран и предложение о создании собственной «Инициативы по безопасности данных», которая «может послужить предварительной основой для обсуждения».

Испания: «Если нам не удастся договориться о глобальных правилах в рамках Организации Объединенных Наций, нынешняя геополитическая напряженность может привести к дроблению киберпространства на различные сферы влияния с

[9] Веб-ТВ ООН, 3-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 14 декабря 2021 года, https://media.un.org/en/asset/k11/k11eljcg88 (начало на отметке 1:14:20)
[10] Веб-ТВ ООН, 3-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 14 декабря 2021 года, https://media.un.org/en/asset/k11/k11eljcg88 (начало на отметке 1:50:40)
[11] Заявление советника У Цзяньцзяня, главы китайской делегации, в ходе общего обмена мнениями на первой основной сессии Рабочей группы открытого состава по безопасности и использованию информационно-коммуникационных технологий, 14 декабря 2021 года, https://documents.unoda.org/wp-content/uploads/2021/12/Statement-of-China_ICT-OEWG-3rd-plenary-meeting_General-Exchange-of-Views_DEC-14-AM_ENG.pdf

несовместимыми друг с другом стандартами сертификации и техническими особенностями».[12]

Китай: «Киберпространство находится под угрозой фрагментации. Генеральный секретарь ООН Гутерриш предупредил на Генеральной Ассамблее этого года, что мир рискует расколоться на две части с двумя противоречащими друг другу наборами стандартов. То же самое можно сказать и о киберпространстве».[13]

Исламская Республика Иран: «Это требует более комплексного подхода к угрозам в сфере информационной безопасности, который касается не только цифровой инфраструктуры, но и самого контента и информации. Примеры срочных и сложных, существующих и потенциальных угроз, с которыми сталкиваются государства: (1) монополия и гегемония в управлении интернетом...»[14]

Контекст. Нет никаких доказательств «монополии и гегемонии» в управлении интернетом. Вопросы управления Интернетом широко обсуждались на ВВУИО и во время переговоров по ВВУИО+10 на Генеральной Ассамблее ООН, и такой вывод не был сделан ни в Тунисской программе ВВУИО, ни в Итоговом документе ВВУИО+10.

15 декабря 2021 года

Нидерланды: «Некоторые примеры существующих вызовов и потенциальных угроз, с которыми сталкивается мировое сообщество, включают кибероперации против целостности, функционирования и доступности интернета, о которых говорится в нормативно-правовых актах. Эта техническая инфраструктура, необходимая для обеспечения общей доступности или целостности Интернета, или общественное ядро, упоминалась как критическая инфраструктура в предыдущих отчетах РГОС и GGE (норма 13f). Эта техническая инфраструктура, необходимая для общего функционирования интернета, также нуждается в защите от попыток контролировать ее таким образом, чтобы подорвать целостность или доступность интернета. Мы видим, что эти тенденции исходят от широкого круга участников. В частности, ни в коем случае нельзя подрывать модель управления интернетом, которая основана на управлении с участием многих заинтересованных сторон. Частный сектор, гражданское общество, техническое сообщество и другие заинтересованные стороны неотъемлемо связаны с функционированием Интернета».[15]

---

[12] Веб-ТВ ООН, 4-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 14 декабря 2021 года, https://media.un.org/en/asset/k1b/k1b55qgp81 (начало на отметке 04:30)

[13] Веб-ТВ ООН, 4-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 14 декабря 2021 года, https://media.un.org/en/asset/k1b/k1b55qgp81 (начало на отметке 1:56:42)

[14] Веб-ТВ ООН, 4-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 14 декабря 2021 года, https://media.un.org/en/asset/k1b/k1b55qgp81 (начало на отметке 2:35:20)

[15] Веб-ТВ ООН, 5-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 15 декабря 2021 года, https://media.un.org/en/asset/k1r/k1royetcr4 (начало на отметке 39:42), а также здесь: Заявление Её Превосходительства Натали Яарсма, специального представителя по вопросам политики безопасности и кибернетики, 15 декабря 2021 года, https://documents.unoda.org/wp-content/uploads/2021/12/21.12.15-Netherlands-Statement-on-Threats-OEWG-in-the-Field-of-Information-and-Telecommunications-in-the-Context-of-Internat.pdf

Исламская Республика Иран: «Мы считаем, что существенное реформирование нынешней системы управления интернетом, открытый справедливый и недискриминационный доступ государств к ИКТ-технологиям и надежная цепочка поставок средств кибербезопасности являются важнейшими требованиями ответственного поведения государств в ИКТ-среде».[16]

Контекст. Рабочая группа по управлению интернетом (WGIG) разработала такое определение управления интернетом: «Управление Интернетом — это разработка и применение правительствами, частным сектором и гражданским обществом, в рамках их соответствующих функций, общих принципов, норм, правил, процедур принятия решений и программ, определяющих развитие и использование Интернета».[17] Соответственно, оно не относится к вопросам, рассматриваемым в заявлении. Текущее состояние управления интернетом ежегодно обсуждается на Форуме по управлению интернетом (IGF), который является подходящей площадкой для таких обсуждений, поскольку в нем может принять участие любой желающий. Будущее состояние управления Интернетом будет обсуждаться в рамках WSIS+20 в 2025 году на Генеральной ассемблее ООН.

Индия: «Нам необходимо обсудить обязательства по непроведению и ответственность за сознательное разрешение атак на публичное ядро интернета. Сюда входят: элементы маршрутизации и пересылки пакетов, системы именования и нумерации, криптографические механизмы безопасности и идентификации, средства передачи, программное обеспечение и центры обработки данных».[18]

16 декабря 2021 года

Коста-Рика: «Передовой опыт и уроки также могут быть позаимствованы у технического сообщества, поскольку группы CERT возглавляют сообщества, которые полагаются на доверительные отношения для обмена информацией при реагировании на события в сфере ИКТ. Мы можем извлечь уроки из того, что важно не просто указывать имена в справочнике, а созывать встречи или проводить упражнения для укрепления доверия и отношений внутри сети».[19]

17 декабря 2021 года

Исламская Республика Иран: «РГОС должна рассмотреть основные источники недоверия в среде ИКТ, в частности, монополию в управлении интернетом, анонимность,

---

[16] Веб-ТВ ООН, 6-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021-2025 — Первая основная сессия, 15 декабря 2021 года, https://media.un.org/en/asset/k1r/k1rnexulnt (начало на отметке 50:35)

[17] Отчет Рабочей группы по управлению Интернетом, июнь 2005 г., пункт 10, https://www.wgig.org/docs/WGIGREPORT.pdf

[18] Веб-ТВ ООН, 6-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021–2025 – Первая основная сессия, 15 декабря 2021 года, https://media.un.org/en/asset/k1r/k1rnexulnt (начало на отметке 01:48:55)

[19] Веб-ТВ ООН, 8-е пленарное заседание, Рабочая группа открытого состава по безопасности и использованию информационно-коммуникационных технологий 2021–2025 – Первая основная сессия, 16 декабря 2021 года, https://media.un.org/en/asset/k1y/k1yzr8yhb1 (начало на отметке: 57:20), а также здесь: Постоянное представительство Коста-Рики при Организации Объединенных Наций, заявление, 16 декабря 2021 года, https://documents.unoda.org/wp-content/uploads/2021/12/Final-Costa-Rica-CBMs-1612021-SP-EN.pdf

наступательные киберстратегии, создание враждебного имиджа и ксенофобию, ведущую к односторонним принудительным мерам, а также отсутствие ответственности частных компаний и платформ и их национальных государств за экстерриториальную деятельность. Например, отправной точкой является реализация многостороннего, справедливого и транспарентного управления интернетом».[20]

Контекст. Нет никаких доказательств «монополии в управлении интернетом». Управление интернетом определено в Тунисской программе ВВУИО, и все заинтересованные стороны, включая правительства, принимают в ней участие. Не существует и доказанного консенсуса в отношении новой, многосторонней модели управления интернетом. Об этом Германия заявила 28 марта 2022 года (см. цитату ниже).

[20] Представление Ирана (Исламская Республика) на первой основной сессии, 17 декабря 2022 года, стр. 8-9, https://documents.unoda.org/wp-content/uploads/2021/12/Irans-submission-to-first-substantive-session_13-17-Dec-21.pdf

Вторая основная сессия

28 марта 2022 года

Заместитель Генерального секретаря ООН Идзуми Накамицу: «Общепризнанно, что в сфере безопасности ИКТ, где частные структуры владеют и управляют большей частью соответствующей инфраструктуры, необходимо взаимодействие многих заинтересованных сторон».[21]

США: «Этот процесс [РГОС] здесь сегодня [...] принадлежит каждому государству-члену, которое стремится сохранить стабильность в киберпространстве, он принадлежит каждой заинтересованной стороне, которая выигрывает от открытого, функционально совместимого, безопасного и надежного интернета для всех...»[22]

Германия: «Интернет не принадлежит государствам и не контролируется ими. Это общественное достояние, которое управляется и развивается очень сложным и эффективным кругом участников, представляющих промышленность, гражданское общество и правительства. Участие в этой Рабочей группе открытого состава должно полностью отражать эту реальность».[23]

Испания: Мы видим реальную угрозу фрагментации в сферах, она может затронуть технические спецификации, которые в итоге окажутся совершенно несовместимыми между собой". Мы не можем допустить, чтобы это произошло, потому что это напрямую затронет все наши страны».[24]

29 марта 2022 года

Российская Федерация: «Например, существует абсолютно реальная возможность того, что целая страна будет отрезана от международных систем связи, в частности, от Интернета или межбанковской системы передачи информации и осуществления платежей SWIFT. Это не теоретическая угроза; это то, что происходит с моей страной. Опыт показывает, что технологии позволяют осуществить эту угрозу, поскольку этими системами управляет одна страна или очень небольшая группа стран. Так, если взять в качестве примера Интернет, то это корпорация по управлению доменными именами и IP-адресами — ICANN. Это международная некоммерческая организация, которая де-факто

[21] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1h/k1hhzc7i5z (начало на отметке 6:27)
[22] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1h/k1hhzc7i5z (начало на отметке 35:00)
[23] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1h/k1hhzc7i5z (начало на отметке 1:13:55), а также здесь: Заявление Германии на мартовской сессии РГОС, пункт 3 повестки дня, 22 апреля 2022 г., стр. 3, https://documents.unoda.org/wp-content/uploads/2022/04/German-Statement-at-the-March-2022-OEWG-Agenda-Item-3.pdf)
[24] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1h/k1hhzc7i5z (начало на отметке 1:52)

полностью контролируется Соединенными Штатами Америки. Эти условия делают любую страну – любую! – уязвимой перед политическими решениями такой страны».[25]

Контекст. ICANN не в состоянии «отключить» (остановить, закрыть и т. д.) какую-либо страну от Интернета. Об этом очень четко говорится в письме президента и генерального директора ICANN от 2 марта 2022 года, адресованном заместителю премьер-министра Украины.[26] Региональная интернет-регистратура для Европы, Ближнего Востока и части Центральной Азии, Европейский сетевой координационный центр IP-сетей RIPE (RIPE NCC) выразили аналогичную позицию в публикации от 10 марта 2022 года.[27] Это также было отмечено 5 апреля 2022 года г-жой Фионой Александер[28]: «Российская Федерация была лучше защищена в мультистейкхолдерной модели, чем в системе ООН. Так что когда украинский министр просил и RIPE, и ICANN отобрать у них интернет-ресурсы, оба ответили «нет».[29] Но в марте 2022 года на Всемирной ассамблее МСЭ по стандартизации в области телекоммуникаций российское правительство по просьбе Украины было лишено руководящих позиций в исследовательских группах.[30] Итак, несмотря на то, что Российская Федерация участвует в ICANN, [она] заявляет о своем желании передать корпорацию под контроль МСЭ или заменить [на что-то другое]. Для меня ирония заключается в том, что модель с участием многих заинтересованных сторон на самом деле защищала народ России и интернет лучше, чем система ООН, в которой российское государство фактически было лишено своей роли».[31] 6 апреля 2022 года Белый дом выпустил информационный бюллетень о санкциях США, Большой семерки и ЕС в отношении России, в котором говорится, в области доступ к интернету не является объектом санкций.[32]

---

[25] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (3-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1l/k1l7rcax4f (начало на отметке 51:05)

[26] Письмо Йорана Марби, президента и генерального директора Интернет-корпорации по присвоению имен и номеров (ICANN), Михаилу Федорову, заместителю премьер-министра, министру цифровой трансформации Украины, 2 марта 2022 года, https://www.icann.org/en/system/files/correspondence/marby-to-fedorov-02mar22-en.pdf

[27] RIPE NCC, Ответ RIPE NCC на запрос правительства Украины, 10 апреля 2022 года, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[28] В настоящее время Фиона Александер занимает пост почетного политтехнолога в Школе международной дипломатической службы и почетного научного сотрудника Лаборатории управления интернетом в Американском университете. Фиона проработала в Национальном управлении по телекоммуникациям и информации (NTIA) Министерства торговли США на посту заместителя администратора по международным вопросам около 20 лет.

[29] Ответ RIPE NCC на запрос правительства Украины. Письмо вице-премьер-министра Украины в RIPE NCC (PDF), ответ управляющего директора RIPE NCC (PDF), Амстердам, 10 марта 2022 года, https://www.ripe.net/publications/news/announcements/ripe-ncc-response-to-request-from-ukrainian-government

[30] Официальный аккаунт в Twitter Постоянного представительства Украины при ООН. Женевский офис, 9 марта 2022 года, https://twitter.com/UKRinUNOG/status/1501658319932600326, сайт Постоянного представительства Чешской Республики при ООН. Женевский офис, 9 марта 2022 года, https://www.mzv.cz/mission.geneva/en/specialized_agencies/international_telecommunication_union/russia_s_military_aggression_against.html

[31] Фиона Александер, вебинар ITIF, Управление интернетом во время войн и конфликтов, 5 апреля 2022 года, (начало на отметке 58:57), https://itif.org/events/2022/04/05/internet-governance-during-times-war-and-conflict

[32] Белый дом, конференц-зал, ИНФОРМАЦИОННАЯ СПРАВКА: Соединенные Штаты, G7 и ЕС налагают на Россию серьезные и немедленные санкции, 6 апреля 2022 года, https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/factsheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/

Малайзия: «В этой связи [мы] могли бы рассмотреть возможность принятия оперативных и эффективных мер со стороны хостинг-провайдера и правоприменительных органов, интернет-провайдеров, регистраторов доменных имен по блокированию и удалению вредоносных сайтов на уровне хостинг-провайдера, на которых необходимо сосредоточиться, особенно на тех, которые влияют на критическую информационную инфраструктуру».[33]

Нидерланды: «Инициативы, наносящие ущерб технической инфраструктуре, необходимой для общей доступности или целостности Интернета, также называемой публичным ядром Интернета, включают кибероперации, направленные на основную физическую и логическую инфраструктуру Интернета, или организации, занимающие центральное место в глобальной маршрутизации, именовании и нумерации, такие как региональные интернет-регистратуры, ICANN и крупные пункты обмена интернет-трафиком. К ним также относятся те, кто внедряет интернет-стандарты и протоколы, подрывающие открытый и функционально совместимый характер Интернета. Для дальнейшего углубления нашего технического понимания публичного ядра Нидерланды инициируют мероприятия по публичному ядру, чтобы углубить наше совместное техническое понимание в сообществе Рабочей группы открытого состава».[34]

Исламская Республика Иран: «Несмотря на риски, связанные с существующей монополией в управлении интернетом, и необходимость создания новой архитектуры, этот вопрос до сих пор не обсуждался в системе ООН после Всемирной встречи на высшем уровне по вопросам информационного общества (ВВУИО), состоявшейся в Тунисе в 2005 году (статьи 29-82 Тунисской программы для информационного общества). К сожалению, Форум по управлению Интернетом (IGF) отказывается обсуждать этот вопрос и передает его на рассмотрение РГОС, в то время как РГОС считает, что обсуждение вопросов управления Интернетом выходит за рамки ее мандата, и передает его на рассмотрение IGF. В результате международное сообщество не смогло достичь консенсуса в отношении глобального управления интернетом, что позволило бы устранить нынешнюю монополию на управление интернетом. Международное сообщество должно в ближайшее время наметить лучшее решение по управлению интернетом в рамках РГОС, которое обеспечит стабильность и безопасность среды ИКТ».[35]

Контекст. Здесь, как и ранее на этой неделе, Иран утверждает, что имеется «существующая монополия в управлении Интернетом», и это мнение не подтверждается фактами. Кроме того, Иран утверждает, что необходима «новая архитектура», но неясно, что это будет за «новая архитектура». Однако вопрос о совершенствовании архитектуры цифрового сотрудничества был рассмотрен в

[33] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (3-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1l/k1l7rcax4f (начало на отметке 1:18:48)

[34] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (3-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1l/k1l7rcax4f (начало на отметке 1:26:20)

[35] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (3-е заседание), вторая основная сессия, 29 марта 2022 года, https://media.un.org/en/asset/k1l/k1l7rcax4f (начало на отметке 1:35:05), а также здесь: Заявление делегации Исламской Республики Иран на второй основной сессии Рабочей группы открытого состава по безопасности и использованию информационных и телекоммуникационных технологий, 29 марта 2022 года, стр. 3, https://documents.unoda.org/wp-content/uploads/2022/03/1-Introductory-Remarks-Existing-and-Potential-Threats.pdf

Дорожной карте цифрового сотрудничества Генерального секретаря ООН. В 2022 году Генеральный секретарь ООН учредил Группу высокопоставленного руководства IGF — многосторонний орган для поддержки и укрепления IGF.[36] *Кроме того, все вопросы, связанные с управлением интернетом, обсуждались с 2003 года в рамках ВВУИО и обзора ВВУИО+10, а также неоднократно на IGF. Иран утверждает, что IGF «отказывается обсуждать этот вопрос», однако IGF активно обсуждает любые вопросы, которые участники выдвинули в виде предложений, принятых Многосторонней консультативной группой IGF. Управление интернетом носит глобальный характер и хорошо описано и объяснено в документах ВВУИО.*[37]

Франция: «Наша делегация хотела бы обратить внимание Группы на угрозы свободному и функционально совместимому характеру киберпространства. В контексте международного внимания мы можем наблюдать растущее обособление киберпространства [...], в том числе на самых глубоких уровнях. [...] Никогда не было санкций в отношении государств, имеющих доступ к глубоким уровням Интернета. Но это искушение обсуждается все чаще и является очень опасным. Такая фрагментация несет в себе риски не только для соответствующих прав человека, свободного распространения информации, экономического роста, но и все больше для международной стабильности. Действительно, если у нас будет несколько разных Интернетов, государства могут решить заняться злонамеренной деятельностью, если почувствуют, что могут сделать это, защищая ненадежный Интернет и имея в дополнение к нему еще один. Наша группа должна принять это во внимание, и это должно побудить нас удвоить наши усилия по сохранению архитектуры свободного киберпространства, которое является единым, открытым, стабильным, безопасным и универсально доступным».[38]

30 марта 2022 года

Нидерланды: «Для Нидерландов защита публичного ядра включает в себя соблюдение принципов модели управления с участием многих заинтересованных сторон и предотвращение внедрения стандартов и протоколов, которые подорвут открытый и функционально совместимый характер Интернета. В этом контексте и в ответ на то, что было предложено вчера, я хотел бы подчеркнуть, что роль таких мультистейкхолдерных организаций, как ICANN и региональные интернет-регистратуры заключается в обеспечении технической координации Интернета и работе по поддержанию единого, глобального и совместимого Интернета, который продолжает работать всегда и доступен для всех...»[39]

---

[36] См. также: Организация Объединенных Наций, Группа высокого уровня Генерального секретаря по цифровому сотрудничеству, https://www.un.org/en/sg-digital-cooperation-panel

[37] Совместное письмо Группы руководства и Многосторонней консультативной группы сокоординаторам GDC, «Форум ООН по управлению Интернетом готов взять на себя ответственность, вытекающую из периодического многостороннего обзора Глобального цифрового договора и последующих действий», 16 октября 2023 года, https://www.intgovforum.org/en/filedepot_download/24/26649

[38] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (3-е заседание), вторая основная сессия, 3-е заседание, 29 марта 2022 года, https://media.un.org/en/asset/k1l/k1l7rcax4f (начало на отметке 15:07)

[39] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), вторая основная сессия, 30 марта 2022 года, https://media.un.org/en/asset/k1g/k1gu15nuh2 (начало на отметке 1:00:07)

Российская Федерация: «Все государства должны играть равную роль в международном управлении интернетом и нести равную ответственность за управление интернетом».[40]

Контекст. Нет никаких доказательств того, что государства не играют «равной роли в международном управлении интернетом» и не несут «равной ответственности» за него.

Китай: «Мы придерживаемся мнения, что государства обладают юрисдикцией в отношении инфраструктуры ИКТ, ресурсов, а также деятельности на их территории. Ни одна страна не должна саботировать критическую инфраструктуру других государств с помощью ИКТ или заниматься уничтожением или кражей важных данных такой инфраструктуры. Государства должны совершенствовать законодательство по защите критических информационных инфраструктур». [...] «С 1 сентября 2021 года в Китае вступило в силу постановление о защите безопасности критической информационной инфраструктуры. Согласно положению, под критической информационной инфраструктурой понимаются важные сети и информационные системы ключевых отраслей и секторов, таких как государственные телекоммуникационные и информационные услуги, энергетика, транспорт, гидротехнические сооружения, финансы, государственная служба, электронное правительство и оборона, наука и технологии. Есть и другие сети и системы, компрометация, потеря работоспособности или утечка данных которых может нанести серьезный ущерб национальной безопасности, экономике страны и общественным интересам. Китай приветствует углубленное обсуждение в рамках РГОС вопроса об определении и защите критической инфраструктуры на основе принципа суверенитета».[41]

Португалия: «Манипуляции с IP в контексте атак на ядро интернета или на целостность избирательных процессов также могут иметь первостепенное значение».[42]

Сингапур: «Одним из примеров критической инфраструктуры могут быть системы технической инфраструктуры, необходимые для обеспечения общей доступности или целостности интернета». [43]

Российская Федерация: На современном этапе развития ИКТ безошибочное определение источника вредоносной деятельности не представляется возможным без глубокой реформы протоколов функционирования глобальной коммуникационной сети и организации необходимого сотрудничества между государствами». В этой связи создание четкого механизма взаимодействия между уполномоченными государственными

[40] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), вторая основная 30 марта 2022 года, https://media.un.org/en/asset/k1g/k1gu15nuh2 (начало на отметке 1:10:18), а также здесь: Заявление главы делегации Российской Федерации В. Шина, 30 марта 2022 г., стр. 3, https://documents.unoda.org/wp-content/uploads/2022/03/Russia-OEWG-statement-3-30.03.2022-Eng.pdf)

[41] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), вторая основная сессия, 30 марта 2022 года, https://media.un.org/en/asset/k1g/k1gu15nuh2 (начало на отметке 1:57:29)

[42] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), вторая основная сессия, 30 марта 2022 года, https://media.un.org/en/asset/k1g/k1gu15nuh2 (начало на отметке 2:06:50)

[43] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), вторая основная сессия, 30 марта 2022 года, https://media.un.org/en/asset/k1g/k1gu15nuh2 (начало на отметке 2:36:05)

органами по типу сотрудничества между группами CERT представляется весьма актуальным».[44]

Контекст. Нет никаких доказательств того, что такая «глубокая реформа [интернета]» необходима для заявленной цели. По всему миру существует бесчисленное множество уголовных дел, в которых правоохранительным органам удавалось установить источник описанной деятельности.[45]

31 марта 2022 года

Канада: «Например, в ОБСЕ мы вместе с Казахстаном выступаем за CBM 4. Его цель — способствовать обмену информацией о национальных подходах к обеспечению открытого, безопасного и функционально совместимого интернета. Эта работа, как мы надеемся, поможет защитить общую доступность и целостность интернета — цель, которую разделяют Нидерланды и другие страны, упоминавшиеся на этой неделе».[46]

Исламская Республика Иран: «Меры по укреплению доверия в киберпространстве (ТСВМ) должны быть встроены в среду ИКТ, чтобы устранить основные источники недоверия в среде ИКТ, в частности монополию в управлении интернетом, анонимность, агрессивные киберстратегии и политику, создание враждебного имиджа и ксенофобию, односторонние принудительные меры и отсутствие ответственности частных компаний, а также платформ и их соответствующих государств за экстерриториальную деятельность.

Мы считаем, что отправной точкой должна стать реализация многостороннего, справедливого и транспарентного управления интернетом. Мы считаем, что монополия (в управлении) и анонимность (людей и вещей) являются основными источниками недоверия в интернете, что обусловливает необходимость соответствующих CBM. В первую очередь необходимо устранить недостатки и негативные стороны существующей системы управления интернетом, чтобы реализовать долгожданное справедливое управление интернетом».[47]

---

[44] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (6-е заседание), вторая основная сессия, 30 марта 2022 года, https://media.un.org/en/asset/k1j/k1jpaw8mgf (начало на отметке 34:40)

[45] См. доклад Министерства внутренних дел Российской Федерации (МВД России) о состоянии преступности в России за январь-ноябрь 2022 года, стр. 3, пункт 9 https://d-russia.ru/wp-content/uploads/2022/12/mvd_22_11_.pdf или отчет ФБР о преступности в интернете за 2022 год, стр. 8, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf или Преступность в Индии, Министерство внутренних дел, Национальное бюро регистрации преступлений, Индия, ТАБЛИЦА 9A.2 Киберпреступления - дела по Закону об информационных технологиях (по главным преступникам и по штатам/округам) - 2021, https://ncrb.gov.in/uploads/nationalcrimerecordsbureau/post/1679661922TABLE9A2.pdf

[46] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (7-е заседание), вторая основная сессия, 31 марта 2022 года, https://media.un.org/en/asset/k1i/k1iykegjsm (начало на отметке 22:40)

[47] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (7-е заседание), вторая основная 31 марта 2022 года, https://media.un.org/en/asset/k1i/k1iykegjsm (начало на отметке 31: 50), а также здесь: Заявление г-на Хейдара Али Балуджи, первого советника Постоянного представительства Исламской Республики Иран при Организации Объединенных Наций, 31 марта 2022 года, стр. 1, https://documents.unoda.org/wp-content/uploads/2022/03/4-CBMs.pdf

Третья основная сессия

25 июля 2022 года

Заместитель Генерального секретаря Идзуми Накамицу: «Я приветствую предложения, связанные с укреплением защиты критической инфраструктуры и критической информационной инфраструктуры, в том числе путем расширения взаимодействия с заинтересованными сторонами по этой теме. Это соответствует требованию Генерального секретаря об установлении приоритетности мер по усилению защиты критической инфраструктуры, включая сектор здравоохранения».[48]

И: «Я неоднократно подчеркивал важность привлечения заинтересованных сторон на инклюзивной и устойчивой основе, учитывая уникальный характер ИКТ и ту центральную роль, которую играют неправительственные организации в управлении многими ресурсами ИКТ».[49]

Европейский Союз: «В списке есть и спорные элементы. Во-первых, предложение согласовать терминологию и список критической инфраструктуры — это пример предложения, которое, по нашему опыту, не позволит достичь консенсуса между государствами. Исходя из опыта предыдущих многосторонних и региональных встреч, эти обсуждения считаются противоречивыми, требуют много времени и могут означать, что в случае со списком объектов критической инфраструктуры они являются приемлемыми целями».[50]

Китай: «На самом деле, что касается тенденции, когда ИКТ-среда становится все более и более разделенной, я думаю, что другие коллеги, присутствующие здесь, знают об этой тенденции и реальности. Генеральный секретарь Гутерриш на двух последовательных общих дебатах в ходе Генеральной Ассамблеи напомнил международному сообществу об угрозе того, что ИКТ-среда становится все более фрагментированной, а киберпространство — все более раздробленным. Таким образом, фрагментация ИКТ-среды имеет непосредственное отношение к нашим рассуждениям. Поэтому, если этот мир разделен или раздроблен на разные части, в нем не будет единого свода правил. Тогда будет невозможно достичь консенсуса по поводу выполнения или применимости международных правил. Не говоря уже о каких-либо мерах по укреплению доверия. Поэтому я надеюсь, что в раздел существующих и потенциальных угроз мы должны включить обсуждение того, как решить самую важную, самую заметную проблему в ИКТ-среде на данный момент».[51]

---

[48] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1u/k1uo46thhm (начало на отметке 05:53)

[49] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1u/k1uo46thhm (начало на отметке 07:54)

[50] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1u/k1uo46thhm (начало на отметке 02:07)

[51] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1u/k1uo46thhm (начало на отметке 02:26)

Испания: **«**Если речь заходит о киберугрозах, мы предлагаем описать их в отчете, отразив существующие проблемы в киберпространстве и проблемы, которые они несут для работы цифрового общества, частных граждан и работы государственных учреждений через технические и нормативные документы, должна быть обеспечена эффективная защита персональных данных, а также интеллектуальной собственности в трансграничных и международных обменах. В Европе действуют Общие положения о защите данных, которые обеспечивают высокий уровень стабильности и безопасности при обмене данными. Чем безопаснее, чем выше эти гарантии защиты — тем выше будет уровень защиты и тем охотнее граждане и предприятия будут обмениваться данными».[52]

Бразилия: **«**Наконец, что касается интерфейсов, — в отчете есть интерфейс с треком управления интернетом, когда мы обсуждаем риски фрагментации, обеспечения доступности и целостности: мы приветствуем эту озабоченность в отчете, но мы хотели бы помнить о надлежащем месте для обсуждения более широких вопросов управления интернетом».[53]

Российская Федерация: «Принципиально важно отразить в первоначальном проекте доклада меры по обеспечению доступности безопасного и стабильного функционирования интернета с акцентом на суверенитет государств в их соответствующем национальном информационном пространстве. И обеспечить равноправное участие государств в управлении этой сетью».[54]

Контекст. Участие государства в управлении Интернетом — вопрос, который обсуждался и решался в ходе ВВУИО. Глобальный интернет состоит из тысяч подключенных сетей, которые находятся в независимом владении и управлении — некоторые из них принадлежат правительствам. Нет никаких доказательств того, что государства не имеют права на «равное участие... в управлении этой сетью».

Российская Федерация: «В вопросе укрепления взаимодействия с негосударственными субъектами в сфере ИКТ-безопасности мы видим преимущество в том, чтобы услышать мнение тех заинтересованных сторон, которые несут прямую ответственность за защиту объекта критической инфраструктуры, в том числе критической информационной инфраструктуры, являясь ее субъектами. Такой диалог должен проходить при понимании ключевой роли национальных правительств в этом вопросе».[55]

---

[52] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (1-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1u/k1uo46thhm (начало на отметке 02:41)

[53] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (2-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1a/k1a978izhq (начало на отметке 7:52), а также здесь: Замечания делегации Бразилии по проекту доклада о ходе работы (разделы: введение, угрозы, нормы), 27 июля 2022 года, стр. 2, https://documents.unoda.org/wp-content/uploads/2022/07/Brazil-part-1.pdf

[54] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (2-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1a/k1a978izhq (начало на отметке 27:10)

[55] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (2-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1a/k1a978izhq (начало на отметке 27:45)

Камерун**: «**Мы считаем, что важно поддерживать государства во всех их возможностях, чтобы заполнить пробелы, а также решить проблемы с IP-адресами».[56]

Нидерланды: «Мы приветствуем ссылку на общую доступность и целостность интернета. В качестве редакционного замечания я бы попросил отразить эту концепцию в отчетах РГОС и ГПЭ за 2021 год. В этих отчетах концепция обозначается как: «техническая инфраструктура, необходимая для обеспечения общей доступности или целостности Интернета».[57]

27 июля 2022 года

Пакистан: «Пакистан горячо поддержал идею CBM и далее рекомендовал шаги, которые призывают к расширению сотрудничества между соответствующими группами CERT государств-членов, которые занимаются расследованиями или соответствующими запросами интернет-протоколов, и к устранению технических препятствий в области кибер-атрибуции».[58]

Первый ежегодный доклад о ходе работы Рабочей группы открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025 гг.

В первом ежегодном докладе о ходе работы РГОС подведены итоги мнений, обсуждений и предложений, выдвинутых на сессии РГОС в 2021-2022 годах. По сути, он стал согласованным документом, подготовившим почву для дискуссий в 2023 году.[59]

8 августа 2022

Первый ежегодный отчет о ходе работы РГОС: «Особую озабоченность вызывает злонамеренная деятельность с использованием ИКТ, затрагивающая критическую информационную инфраструктуру, инфраструктуру предоставления социально значимых услуг населению, техническую инфраструктуру, необходимую для обеспечения

[56] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (2-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1a/k1a978izhq (начало на отметке 43:42)
[57] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (2-е заседание), третья основная сессия, 25 июля 2022 года, https://media.un.org/en/asset/k1a/k1a978izhq (начало на отметке 1:31:53)
[58] Веб-ТВ ООН, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021–2025 (5-е заседание), третья основная сессия, 27 июля 2022 года, https://media.un.org/en/asset/k10/k100qzajqy (начало на отметке 8:35)
[59]Доклад рабочей группы открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, Итоговые отчеты, 22 августа 2022 года, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports

общедоступности или целостности интернета, а также для работы организаций из сектора здравоохранения».

Контекст. Приведенная выше формулировка взята из отчета Группы правительственных экспертов ООН за 2021 год.[60]

Первый ежегодный отчет о ходе работы РГОС: «Государства могли бы укреплять координацию и сотрудничество между государствами и заинтересованными сторонами, включая бизнес, неправительственные организации и сектор науки и образования. Государства отметили, что заинтересованные стороны уже играют важную роль, налаживая партнерские отношения с государствами в целях обучения, проведения исследований и облегчения доступа к интернету и цифровым услугам». [61] [62]

Неофициальные консультации

Председатель РГОС провел несколько неофициальных консультаций между собраниями. Приведенные ниже цитаты взяты из материалов, опубликованных на сайте РГОС.

7 декабря 2022 года Россия представила следующее заявление в рамках неофициальных консультаций РГОС: «На современном этапе развития ИКТ достоверное и однозначное определение источника вредоносной активности невозможно без кардинального реформирования протоколов глобальной сети связи и организации необходимого межгосударственного взаимодействия. В связи с этим создание четких механизмов взаимодействия между компетентными государственными органами становится особенно необходимым».[63]

Контекст. Российская Федерация не представила никаких доказательств того, что для достижения описанной цели необходимо «кардинально реформировать протоколы» интернета. Общепринятые интернет-протоколы, такие как протокол управления передачей/интернет-протокол (TCP/IP), обеспечивают связь между устройствами. Инженерная проектная группа Интернета (IETF) отвечает за набор

[60] Доклад ГПЭ 2021 года, A/76/135, согласованная резолюция ГА 76/19, 14 июля 2021 года, пункт 10, https://documents.un.org/prod/ods.nsf/xpSearchResultsM.xsp

[61] Первый ежегодный доклад о ходе работы Рабочей группы открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, 8 августа 2022, стр. 13, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N22/454/03/PDF/N2245403.pdf?OpenElement

[62] Представители Российской Федерации и Украины заблокировали участие некоторых неправительственных организаций в работе РГОС. В общей сложности 32 организации были исключены из предложенного списка аккредитации# на сессиях РГОС, поскольку государства-члены ранее достигли консенсуса по условиям участия неправительственных организаций. В консенсусе было особо отмечено, что организации, не аккредитованные при ЭКОСОС, смогут участвовать в работе РГОС при условии отсутствия возражений. Украина возражала против участия пяти организаций из России. Россия возражала против участия 10 организаций из США, четырех организаций из Великобритании, трех международных организаций, двух организаций из Германии и по одной организации соответственно из Австралии, Финляндии, Франции, Ирландии, Нигерии, Испании, Швейцарии и Уганды.

[63] Заявление представителя Российской Федерации на неофициальном межсессионном заседании Рабочей группы открытого состава по безопасности и использованию ИКТ 2021-2025 гг., Нью-Йорк, 7 декабря 2022 г., стр. 1, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

протоколов TCP/IP. Любые изменения в пакете TCP/IP регулируются IETF, которая открыта для участия всех желающих.

В том же заявлении Россия добавила: «Не существует общепризнанных норм в области противодействия использованию ИКТ в террористических и преступных целях, пресечения распространения незаконного контента и подделок, а также интернационализации управления интернетом».[64]

Контекст. Существуют уже упомянутые общепризнанные документы — Тунисская повестка дня ВВУИО и Итоговый документ ВВУИО+10, — которые объясняют и подтверждают мультистейкхолдерную модель управления интернетом как результат подлинно международных усилий.

Четвертая основная сессия[65]

7 марта 2023 года Сингапур заявил: «Мы также напоминаем о содержащихся в приложении к резюме Председателя предложениях по защите технической инфраструктуры, необходимой для обеспечения общей доступности или целостности интернета. Такая техническая инфраструктура предполагает наличие DNS — системы доменных имен или пунктов обмена интернет-трафиком, что важно как для развитых, так и для развивающихся стран, учитывая растущую зависимость всех государств от технологий на базе ИКТ. Мы поддерживаем дальнейшее обсуждение в рамках РГОС возможных мер, которые могут быть приняты для обеспечения доступности или целостности Интернета».[66]

Пятая основная сессия

27 июля 2023 года Португалия, среди прочего, рассказала о четырех пунктах, которые не попали в годовой отчет РГОС: «…3. Подтверждение того, что основные службы и критическая инфраструктура всегда должны быть недоступны для вредоносной кибер-активности, 4. Признание важной роли всех заинтересованных сторон, включая технологическую платформу, в каждом компоненте концепции, а именно в ... защите критической инфраструктуры...».[67]

---

[64] Заявление представителя Российской Федерации на неофициальном межсессионном заседании Рабочей группы открытого состава по безопасности и использованию ИКТ 2021-2025 гг., Нью-Йорк, 7 декабря 2022 г., стр. 2, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Russia_-_statement_on_international_law_-_OEWG_intersessionals_07.12.2022.pdf

[65] Некоторые заявления, сделанные в ходе четвертой основной сессии РГОС, содержали повторяющиеся цитаты, которые уже приводились в нашем отчете.

[66] Веб-ТВ ООН, Рабочая группа открытого состава по информационных и коммуникационных технологий (ICT) (3-е заседание) — четвертая основная сессия,7 марта 2023 года (начало на отметке 2:11:30), https://media.un.org/en/asset/k1a/k1ah2cv3gr

[67] Веб-ТВ ООН, Рабочая группа открытого состава по информационных и коммуникационных технологий (ICT) (8-е заседание) — пятая основная сессия, 27 июля 2023 года (начало на отметке 2:11:52), https://media.un.org/en/asset/k1n/k1ngmoogyi

28 июля 2023 года Россия процитировала декларацию саммита Россия-Африка по ИКТ[68] и сделала следующее заявление: «Мы отмечаем необходимость усиления координации между Российской Федерацией и африканскими государствами в международных организациях в рамках системы ООН, когда речь идет о почтовых услугах, и МСЭ. В частности, когда речь идет о разработке документов для развития ИКТ. Мы исходим из того, что Тунисская программа для информационного общества должна быть разработана. Она была принята на форуме ВВУИО в 2005 году. Мы поддерживаем создание сбалансированной международной системы управления интернетом под эгидой ООН, чтобы избежать любых односторонних политических ограничений или коммерческих интересов и обеспечить безопасность и стабильность критической информационной инфраструктуры всемирной паутины».[69]

Контекст. Нет никаких свидетельств того, что имело место какое-либо ограничение, угрожающее «безопасности и стабильности критической информационной инфраструктуры всемирной паутины». Кроме того, нет никаких свидетельств того, что существующая международная система управления интернетом не является сбалансированной или что ее необходимо перевести под эгиду какой-либо межправительственной организации, включая Организацию Объединенных Наций. Фактически Российская Федерация участвует в этой самой системе в качестве члена Правительственного консультативного комитета ICANN.[70]

28 июля 2023 года РГОС приняла 2-й проект годового отчета о ходе работ.[71] В докладе содержалась следующая формулировка:

«Государства также подчеркнули, что направленная против CI и CII злонамеренная деятельность с использованием ИКТ, которая подрывает доверие к политическим и избирательным процессам, государственным учреждениям или оказывает негативное воздействие на общедоступность или целостность интернета, также является реальной и все более серьезной проблемой. Государства выразили особую озабоченность по поводу злонамеренной деятельности в сфере ИКТ, направленной на вмешательство во внутренние дела государств».[72]

«Государства подчеркнули важность защиты критической инфраструктуры (CI) и критической информационной инфраструктуры (CII). Государства подчеркнули, что деятельность ИКТ, которая намеренно наносит ущерб CI или CII или иным образом

[68] Декларация Второго российско-африканского саммита по сотрудничеству в области международной информационной безопасности 28 июля 2023 года, пункт 7, http://en.kremlin.ru/supplement/5975
[69] Веб-ТВ ООН, Рабочая группа открытого состава по информационных и коммуникационных технологий (ICT) (10-е заседание) — пятая основная сессия, 28 июля 2023 года (начало на отметке 11:00), https://media.un.org/en/asset/k1s/k1san5j55u
[70] ICANN | GAC, Правительственный консультативный комитет, https://gac.icann.org/
[71] Доклад рабочей группы открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, Итоговые отчеты, 1 августа 2023 года, https://meetings.unoda.org/meeting/57871/documents?f%5B0%5D=document_type_meeting%3AFinal%20reports
[72] Рабочая группа открытого состава по безопасности и использованию информационных и коммуникационных технологий 2021-2025, пятая основная сессия, Нью-Йорк, 24-28 июля 2023 года, второй годовой отчет о ходе работ, стр. 6, https://documents-dds-ny.un.org/doc/UNDOC/LTD/N23/227/59/PDF/N2322759.pdf?OpenElement

препятствует использованию и функционированию CI или CII для предоставления услуг населению, может иметь каскадные внутренние, региональные и глобальные последствия. Она представляет собой повышенный риск нанесения вреда населению и может носить эскалационный характер. Таким образом, государства подчеркнули необходимость дальнейшего усиления мер по защите всех CI и CII от угроз ИКТ и предложили расширить обмен передовым опытом в области защиты CI и CII, включая обмен национальной политикой, и восстановления после инцидентов с ИКТ, затрагивающих CI и CII. В этой связи государства сослались на резолюцию 58/199 Генеральной Ассамблеи «Формирование глобальной культуры кибербезопасности и защита критических информационных инфраструктур» и сопроводительное приложение к ней. Государства также предложили оказывать поддержку развивающимся странам и малым государствам в определении национальных CI и CII, где это необходимо».[73]

В годовом отчете о ходе работ также содержится следующая рекомендация: «На шестой, седьмой и восьмой сессиях РГОС государства также проведут целенаправленные обсуждения по следующим вопросам: (a) усиление мер по защите CI и CII от угроз со стороны ИКТ, включая обмен передовым опытом в области обнаружения, защиты, реагирования и восстановления после инцидентов в сфере ИКТ, а также оказание поддержки развивающимся странам и малым государствам в идентификации национальных CI и CII, где это необходимо; и (b) дальнейшее сотрудничество и помощь в обеспечении целостности цепочки поставок и предотвращении использования вредоносных скрытых функций».[74]

[73] Тот же источник, стр. 8
[74] Тот же источник, стр. 9

Специальный комитет ООН разработает всеобъемлющую международную конвенцию о противодействии использованию информационных и коммуникационных технологий в преступных целях (АНС)[75]

Первая сессия (материалы, связанные с первой сессией АНС)[76]

29 июня 2021 года

Российская Федерация: «Критическая информационная инфраструктура» — это совокупность объектов критической информационной инфраструктуры и телекоммуникационных сетей, используемых для объединения объектов критической информационной инфраструктуры; n) «объекты критической инфраструктуры» — информационные системы и информационно-коммуникационные сети органов государственной власти, а также информационные системы и автоматизированные системы управления технологическими процессами, функционирующие в сфере обороны, здравоохранения, образования, транспорта, связи, энергетики, банковского и финансового секторов, атомной энергетики и других важных для жизни государства и общества сферах».[77]

8 ноября 2021 года

Интерпол: «Доступ правоохранительных органов к важной регистрационной информации о доменных именах (данные WHOIS) в нынешней нормативной среде ограничен. Чтобы поддержать правоохранительные органы во всем мире в решении этой ключевой задачи, Интерпол разработал и запустил пилотное тестирование нового портала ограниченного доступа, предоставляющего автоматизированный доступ к информации о регистрации доменов для проверенных правоохранительных органов. После успешного завершения пилотной фазы системы Интерпол интегрирует это решение в свой глобальный

[75] Эта глава содержит цитаты из 6 сессий Специального комитета экспертов открытого состава (АНС) и построена таким образом, чтобы отразить вклад в работу Первой и Второй сессий. Цитаты из Третьей сессии также включают в себя записи дискуссий, которые проходили в зале заседаний АНС. На четвертой и пятой сессиях был опубликован проект текста под названием «сводный обсуждаемый документ», а на шестой сессии — «проект текста конвенции». В этой главе приведены соответствующие цитаты из этих документов. См. здесь: Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, Заседания Специального комитета: сессии, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/home

[76] Первая сессия Специального комитета, Нью-Йорк, 28 февраля - 11 марта 2022 года, заявления государств-членов на первой сессии Специального комитета, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-first-session.html

[77] Конвенция Организации Объединенных Наций о противодействии использованию информационных и коммуникационных технологий в преступных целях, проект, неофициальный перевод, Заявление Российской Федерации на первой сессии Специального комитета, 29 июня 2021 года, стр. 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Comments/RF_28_July_2021_-_E.pdf

полицейский потенциал, заключив необходимые юридические соглашения, чтобы расширить круг частных операторов и открыть систему для стран-членов».[78]

Вторая сессия (материалы, связанные со второй сессией AHC)[79]

7 апреля 2022 года

Российская Федерация (от имени Беларуси, Бурунди, Китая, Никарагуа и Таджикистана): «Каждое государство-участник принимает такие законодательные и другие меры, которые могут быть необходимы для наделения его компетентных органов полномочиями отдавать распоряжения: [...] (b) Поставщик услуг, предлагающий свои услуги на территории этого государства-участника, должен представить информацию об абонентах, находящуюся во владении или под контролем этого поставщика услуг». [...] «Для целей настоящей статьи термин "информация об абоненте" означает любую имеющуюся у поставщика услуг информацию, касающуюся абонентов его услуг, за исключением данных о трафике или данных о контенте, на основании которой можно установить: "b) личность абонента, почтовые или иные адреса, телефонные и иные номера доступа, включая IP-адреса, а также биллинговая и платежная информация, имеющаяся в соглашении или договоренности об оказании услуг; c) информация, касающаяся местонахождения информационного и телекоммуникационного оборудования, имеющая отношение к соглашению или договоренности об оказании услуг».[80]

8 апреля 2022 года

Бразилия: «(i) "Данные об абоненте" означает любые компьютерные данные, собранные в ходе обычной деятельности поставщика услуг, относящиеся к имени, дате рождения, почтовому или географическому адресу, биллингу и платежным данным, идентификаторам устройств, номеру телефона или адресу электронной почты, или любой другой информации, такой как IP-адрес, использованный во время создания учетной записи, которая может служить для идентификации абонента или клиента, а также типа предоставляемых услуг и продолжительности контракта с поставщиком услуг, кроме данных о трафике или контенте».[81]

---

[78] Вклад Интерпола в разработку Всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, Заявление Интерпола на первой сессии Специального комитета, 8 ноября 2021 года, стр. 6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/IGOs/21COM1175-SRIUN_UseInformation_CriminalPurposes_complet.pdf

[79] Вторая сессия Специального комитета, Вена, 30 мая - 10 июня 2022 года, Предложения, связанные с второй сессией Специального комитета, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc-second-session.html

[80] Заявление Российской Федерации, также от имени Беларуси, Бурунди, Китая, Никарагуа и Таджикистана, на второй сессии Специального комитета, 7 апреля 2022 года, стр. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Russia_Contribution_E.pdf

[81] Предложение Бразилии по первоначальным главам конвенции Организации Объединенных Наций о киберпреступности, Заявление Бразилии на второй сессии Специального комитета, 8 апреля 2022 года, стр. 2, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Brazil_Contribution_E.pdf

Исламская Республика Иран: «В конвенции должны быть указаны и прописаны обязательства и правила сотрудничества частного сектора, поставщиков услуг и других подобных организаций с правоохранительными органами, в особенности секторов и поставщиков, имеющих глобальный или значительный охват на международном уровне».[82]

Япония: «Кибербезопасность и управление Интернетом не должны рассматриваться в этой конвенции. Например, следующие меры окажут тормозящее воздействие на законную экономическую деятельность и будут препятствовать развитию технологий, а также выйдут за рамки мандата Специального комитета:

- установление стандартов безопасности в соответствии с этой конвенцией;
- возложение на юридические и физические лица обязанностей по соблюдению таких стандартов или установление санкций за нарушение таких стандартов; или
- привлечение к ответственности юридических лиц, их представителей или создателей программного обеспечения, которые непреднамеренно участвуют в киберпреступлениях, совершаемых другими субъектами, не осознавая этого».[83]

9 апреля 2022 года

Канада: Предложено определение «компьютерных данных» как «любого представления фактов, информации или концепций в форме, пригодной для обработки в компьютерной системе, включая программу, пригодную для того, чтобы заставить компьютерную систему выполнить какую-либо функцию». Это определение включает в себя все типы данных: данные о содержимом (собственно сообщение), компьютерные программы, данные о трафике, информацию об абонентах, пароли и коды соединений. Согласно тому же документу, «данные о трафике» означают «любые компьютерные данные для идентификации, активации или настройки устройства, связанного с созданием, передачей или приемом сообщения с помощью компьютерной системы, генерируемые компьютерной системой, которая является частью цепи связи, с указанием происхождения, назначения или прекращения сообщения, маршрута, времени, даты, размера, продолжительности или типа базовой услуги. Это определение включает в себя, как для телефонии, так и для интернет-услуг, данные, необходимые для набора, маршрутизации и адресации или сигнализации, например: телефонные номера, дату и время звонка (и другие элементы в журналах данных звонков), источник и место назначения сообщений (например, происхождение, место назначения или завершения сообщения, маршрут, время, дата, размер, продолжительность или тип базовой услуги. электронная почта или текстовые сообщения), а также IP-адреса и данные, относящиеся к используемому протоколу».[84]

---

[82] Заявление Исламской Республики Иран на второй сессии Специального комитета, 8 апреля 2022 года, стр. 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Islamic_Republic_of_Iran_contribution.pdf

[83] Япония, Предложение по криминализации, общим положениям, процессуальным мерам и правоприменению, Заявление Японии на второй сессии Специального комитета, 8 апреля 2022 года, стр. 5-6, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Japan_Contribution.pdf

[84] Канада, Представление проекта текста и предложений по конкретным главам и положениям, подлежащим рассмотрению на второй сессии Специального комитета, а именно: криминализация, общие положения, процессуальные меры и правоприменение, 9 апреля 2022 года, стр. 1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Canada_Contribution.pdf

12 апреля 2022 года

Вьетнам: Предложено определение киберпространства как «сети инфраструктуры информационных технологий (ИТ), включающей телекоммуникационные сети, интернет, компьютерные сети, системы связи, системы обработки информации и управления, базы данных».[85]

13 апреля 2022 года
Мексика: «Мексика считает, что необходимо добавить другие общие положения по следующим вопросам: [...] признание общественного значения интернета и актуальности подхода, основанного на сетевом нейтралитете, для целей конвенции».[86]

14 апреля 2022 года:
ЮАР: «Каждое государство-участник ведет реестр с идентифицируемой информацией обо всех регистраторах доменных имен, торговцах криптоактивами и криптоактивах, находящихся под его юрисдикцией, в соответствии с основополагающими принципами своего внутреннего законодательства, и предоставляет такую информацию компетентным органам для следственных и доказательственных целей».[87]

Третья сессия (материалы, связанные с третьей сессией AHC)[88]

29 августа 2022

Исламская Республика Иран: «Частные структуры, такие как поставщики услуг, в том числе в области доменных имен, играют особенно важную роль в борьбе с преступлениями, совершаемыми с помощью ИКТ. Учитывая широкие масштабы преступного использования предоставляемых услуг, сотрудничество таких организаций с правоохранительными органами и их должная осмотрительность в этой области, особенно организаций, имеющих значительный охват и осуществляющих деятельность на международном уровне, остается жизненно важным. В связи с этим в Конвенции должны быть прописаны правила и обязательства по эффективному сотрудничеству этих организаций с правоохранительными органами. Кроме того, такие организации должны уважать экономические, социальные, правовые и культурные особенности государств».[89]

---

[85] Предложение Вьетнама на второй сессии Специального комитета, 12 апреля 2022 г., стр. 1, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Vietnam_Contribution.pdf
[86] Предложение правительства Мексики для рассмотрения Специальным комитетом на его второй основной сессии, 13 апреля 2022 года, стр. 3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Mexico_Contribution.pdf
[87] Предложение Южной Африки по положениям о криминализации, общим положениям и положениям о процессуальных мерах и правоприменении, 14 апреля 2022 года, стр. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/South_Africas_contribution.pdf
[88] Третья сессия Специального комитета, 29 августа - 9 сентября 2022 года, Нью-Йорк, Предложения, связанные с третьей сессией Специального комитета, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_third_session/main.html
[89] Веб-ТВ ООН, (1-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 29 августа 2022 года (начало на отметке 1:08:56), https://media.un.org/en/asset/k1x/k1xh926qrt

Китай: «Государства не должны в нарушение законов государства, где хранятся данные, напрямую собирать данные, хранящиеся в иностранных государствах, у предприятий или частных лиц или с помощью технических средств, минуя меры защиты сетевой безопасности».[90]

Канада: «Хотя Канада не возражает против включения статьи 32 в Будапештскую конвенцию, мы считаем, что достижение консенсуса по такой статье может оказаться непосильной задачей, учитывая сжатые сроки, в которые мы работаем над этой конвенцией, и учитывая, что эта статья стала результатом длительных обсуждений».[91]

Контекст. Статья 32 Будапештской конвенции о киберпреступности, касающаяся трансграничного доступа к хранящимся компьютерным данным с согласия или в открытом доступе, гласит следующее:

«Сторона может без разрешения другой Стороны:

a. получать доступ к общедоступным (с открытым исходным кодом) компьютерным данным, независимо от географического местонахождения этих данных; или

получать доступ или получать через компьютерную систему на своей территории хранящиеся компьютерные данные, находящиеся у другой Стороны, если Сторона получает законное и добровольное согласие лица, имеющего законные полномочия на раскрытие данных Стороне через эту компьютерную систему...».[92]

Чили: «Но помимо улик, для любого преступления нужны основные доказательства, и к ним относится интернет или любая другая процедура, подключенная к Сети, которая может быть использована для поддержки преступления или нет».[93]

1 сентября 2022 года

Эквадор: «В связи с этим Эквадор определил несколько потребностей. Их будет слишком много, чтобы привести их все, но в качестве примера я могу упомянуть текущие проблемы с ISP — интернет-провайдерами, поскольку они не хотят иметь адреса IPv4 и вынуждены использовать такие протоколы, как CGNET, который позволяет тысячам пользователей использовать один и тот же публичный IP-адрес. Это затрудняет определение того, кто совершил киберпреступление. И в этой связи мы просим включить в будущую Конвенцию положение, обязывающее государства-участники организовать свои внутренние нормы, чтобы просить интернет-провайдеров в течение разумного

[90] Веб-ТВ ООН, (1-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 29 августа 2022 года (начало на отметке 2:13:22), https://media.un.org/en/asset/k1x/k1xh926qrt
[91] Веб-ТВ ООН, (2-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 29 августа 2022 года (начало на отметке 1:43:42), https://media.un.org/en/asset/k1j/k1jbh2v1z7
[92] Совет Европы, Серия европейских договоров — № 185, Конвенция о киберпреступности, Будапешт, 23 ноября 2001 года, стр. 17, https://rm.coe.int/1680081561
[93] Веб-ТВ ООН, (2-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 29 августа 2022 года (начало на отметке 2:37:05), https://media.un.org/en/asset/k1j/k1jbh2v1z7

периода времени полностью перейти с протокола IPv4 на IPv6. Это позволит добиться благоприятных результатов в расследовании киберпреступлений и, следовательно, удовлетворить требования технической помощи в этой области».[94]

Председатель прокомментировал этот вопрос: «Мы с вами видим, что существуют разнообразные различия с IP-адресами, и это дает нам большой простор для прогресса, и позволяет нам увидеть, что на уровнях технического понимания существуют огромные различия».[95]

Оман: «Я присоединяюсь к заявлению представителя Эквадора о важности обмена рабочими механизмами и перехода от 4-го протокола к 6-му. Это окажет положительное влияние [...] на борьбу с киберпреступностью. Когда компании или поставщики услуг изменят протокол, по которому они работают, — я имею в виду 6-й протокол, — это окажет гораздо большее влияние на борьбу с киберпреступностью».[96]

7 сентября 2022 года

Пакистан: «Пакистан всегда поддерживал идею CBM и далее предлагает следующие рекомендуемые действия, которые призывают к расширению сотрудничества между соответствующими группами реагирования на инциденты информационной безопасности (CERT) государств-членов для решения вопросов расследования / отслеживания интернет-протоколов и устранения технических препятствий на пути кибер-атрибуции».[97]

Россия: «Российская Федерация предложила добавить в документ (доклад) следующие пункты: [...] Государства отмечают важность принятия мер по обеспечению общей доступности, безопасного и стабильного функционирования Интернета с учетом суверенитета государств в их информационном пространстве, а также по обеспечению равного участия государств в управлении этой сетью».[98]

Контекст. Как и в выступлениях в РГОС, Россия не приводит доказательств неравенства участия государств в управлении интернетом. Как объяснялось выше, Российская Федерация является членом GAC ICANN и как таковой наравне со всеми другими членами GAC участвует в работе ICANN.

---

[94] Веб-ТВ ООН, (8-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 1 сентября 2022 года (начало на отметке 1:54:12), https://media.un.org/en/asset/k1o/k1o39wyquf

[95] Веб-ТВ ООН, (8-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 1 сентября 2022 года (начало на отметке 1:58:09), https://media.un.org/en/asset/k1o/k1o39wyquf

[96] Веб-ТВ ООН, (8-е заседание) Третья сессия, Специальный комитет по противодействию использованию ИКТ в преступных целях, 1 сентября 2022 года (начало на отметке 2:06:20), https://media.un.org/en/asset/k1o/k1o39wyquf

[97] Сборник заявлений в порядке разъяснения позиции по вопросу о принятии очередного доклада рабочей группы открытого состава, содержащегося в документе A/77/275, приложение, 7 сентября 2022 года, стр. 26, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

[98] Сборник заявлений в порядке разъяснения позиции по вопросу о принятии очередного доклада рабочей группы открытого состава, содержащегося в документе A/77/275, приложение, 7 сентября 2022 года, стр. 37, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg-II/documents/compendium_2022.pdf

Четвертая[99] и пятая сессии[100] АНС.

Сводный обсуждаемый документ АНС:

Сводный обсуждаемый документ со статусом «по состоянию на 21 апреля 2023 года» был опубликован после Пятой сессии АНС. Обсуждаемый документ содержал проект текста конвенции ООН о киберпреступности, подготовленный председателем Специального комитета. Не все предложения были приняты делегациями, и в текст проекта конвенции были внесены дополнения. Однако мы приводим этот текст здесь, поскольку он имеет отношение к делу.

21 апреля 2023 года

Сводный обсуждаемый документ:

Индия, Пакистан, США, Китай, Новая Зеландия, Египет, Кения, Судан, Австралия, Россия, Колумбия, Норвегия, Канада, Танзания, Сирийская Арабская Республика, Алжир, Буркина-Фасо, Сингапур, ЮАР, Никарагуа, Макао, Тонга, Европейский союз и государства-члены, а также Фиджи заявили, что они хотят исключить проект статьи 72 о «трансграничном доступе к хранимым [компьютерным данным] [электронной/цифровой информации] с согласия или при наличии открытого доступа» из Сводного обсуждаемого документа по преамбуле, положениях о международном сотрудничестве, превентивных мерах, технической помощи и механизме осуществления, а также заключительные положения всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях. Две страны — Эквадор и Венесуэла — высказались за сохранение текста этой статьи после редактирования.[101] Полный текст статьи гласит:

«Государство-участник может без разрешения другого государства-участника:
(a) получать доступ к общедоступным (открытым источникам) хранящимся [компьютерным данным] [электронной/цифровой информации], независимо от географического местонахождения [данных] [информации]; или
(b) получать доступ или получать через [компьютерную систему] [систему/устройство информационных и коммуникационных технологий] на своей территории хранящиеся [компьютерные данные] [электронную/цифровую информацию], находящиеся в другом Государстве-участнике, если Государство-участник, получающее доступ или получающее [данные] [информацию], получает законное и добровольное согласие лица, имеющего

[99] В этой главе нет цитат из Четвертой сессии Специального комитета. Для справки: Четвертая сессия Специального комитета, 9-20 января 2023 года, Вена, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fourth_session/main.html
[100] Пятая сессия Специального комитета, 11-21 апреля 2023 года, Вена, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_fifth_session/main
[101] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, пятая сессия 11 - 21 апреля 2023 года, Сводный обсуждаемый документ по преамбуле, положениям о международном сотрудничестве, превентивных мерах, технической помощи и механизме осуществления и заключительным положениям всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, стр. 38, 21 апреля 2023 года, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/5th_session/Documents/CND_2_-_21.04.2023.pdf

законные полномочия на раскрытие [данных] [информации] этому Государству-участнику через эту компьютерную систему».[102]

Малайзия, Ангола и Намибия предпочли исключить только часть «b)» проекта статьи.

Комментарий: Предварительный экземпляр проекта конвенции, подготовленный для 6-й сессии АНС, не содержал проекта статьи «Статья 72 о трансграничном доступе к хранящимся [компьютерным данным] [электронной/цифровой информации] с согласия или при наличии открытого доступа», аналогичной статье 32 Будапештской конвенции о киберпреступности.[103]

Шестая сессия АНС.[104]

Работа шестой сессии АНС завершилась 1 сентября 2023 года.

Проект текста конвенции (версия по состоянию на 2 сентября 2023 года)

На шестой сессии АНС был подготовлен 80-страничный текст проекта конвенции о киберпреступности. Мы хотели бы обратить ваше внимание на следующие положения этого текста и прокомментировать некоторые из них.

«Статья 2. Использование терминов.

[...]

(c) «Данные о трафике» означают любые [компьютерные данные] [цифровую информацию], собранные поставщиком услуг, за исключением данных о контенте, относящихся к перечисленному ниже: (i) Тип предоставленной услуги и ее продолжительность, если это касается технических данных и данных, идентифицирующих соответствующие технические меры или интерфейсы, используемые или предоставляемые абоненту или клиенту, и данных, связанных с подтверждением использования услуги, за исключением паролей или других средств аутентификации, используемых вместо пароля, которые предоставлены пользователем или созданы по запросу пользователя; (ii) начало и окончание сеанса доступа пользователя к услуге, например, дата и время использования, вход в услугу и выход из нее; и (iii) метаданные связи, обрабатываемые в сети электронных коммуникаций для целей передачи, распространения или обмена данными о содержании, включая данные, используемые для отслеживания и идентификации источника и пункта назначения сообщения, данные о

[102] Тот же источник
[103] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, шестая сессия, 21 августа - 1 сентября 2023 года, проект конвенции (предварительная копия), https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf
[104] Шестая сессия Специального комитета, 21 августа - 1 сентября 2023 года, Нью-Йорк, https://www.unodc.org/unodc/en/cybercrime/ad_hoc_committee/ahc_sixth_session/main

местонахождении оконечного оборудования, используемого в контексте предоставления услуг связи, а также дату, время, продолжительность и тип сообщения;».[105]

Комментарий: Это отличается от определения, содержащегося в Будапештской конвенции о киберпреступности. Согласно Будапештской конвенции: «"данные о трафике" означают любые компьютерные данные, относящиеся к сообщению с помощью компьютерной системы, генерируемые компьютерной системой, которая является частью цепи связи, указывающие на происхождение, место назначения, маршрут, время, дату, размер, продолжительность или тип базовой услуги сообщения».[106]

Будапештская конвенция о киберпреступности содержит те же определения «поставщика услуг» и «информации об абоненте»,[107] но не содержит определения «данных о контенте». Оно представлено в проекте конвенции ООН.[108]

[...]

Доминиканская Республика добавила проект положения к «Статье 2. Использование терминов». Она хочет определить, кто такие «соответствующие заинтересованные[109] стороны».

Российская Федерация, Иран, Беларусь, Буркина-Фасо, Венесуэла, Египет: «Статья 10-бис. Незаконное вмешательство в критическую информационную инфраструктуру. 1. Каждое государство-участник принимает такие законодательные и иные меры, которые необходимы для квалификации в качестве преступления в соответствии с его внутренним законодательством преднамеренного создания, распространения и/или использования программного обеспечения или другой цифровой информации, заведомо предназначенных для незаконного вмешательства в работу критической информационной инфраструктуры, включая программное обеспечение или другую цифровую информацию для уничтожения, блокирования, модификации, копирования содержащейся в них информации или для нейтрализации средств защиты. 2. Каждое

[105] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, шестая сессия, 21 августа - 1 сентября 2023 года, проект текста конвенции (состояние на 2 сентября 2023 года с обновлениями от государств-членов), стр.3, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[106] Совет Европы, Конвенция о киберпреступности, Будапешт, 23 ноября, стр. 3, https://rm.coe.int/1680081561

[107] Совет Европы, Серия европейских договоров — № 185, Конвенция о киберпреступности, Будапешт, 23 ноября 2001 г., стр. 3 и 9, https://rm.coe.int/1680081561

[108] «(d) "Данные о контенте" означают любые [компьютерные данные] [цифровую информацию], относящиеся к сообщению посредством [компьютерной системы] [устройства информационно-коммуникационных технологий], касающиеся сути или цели этого сообщения, такие как текст, голосовые сообщения, аудиозаписи, видеозаписи и другие виды информации». Европейская конвенция о защите физических лиц при автоматизированной обработке персональных данных содержит определение «персональных данных» — термин, который имеет аналогичную формулировку в тексте проекта конвенции ООН: "Персональные данные" означают данные, относящиеся к идентифицированному или идентифицируемому физическому лицу». Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, шестая сессия, 21 августа - 1 сентября 2023 года, проект текста конвенции (состояние на 2 сентября 2023 года с обновлениями от государств-членов), стр. 3- 4, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[109] Тот же источник, стр. 4

государство-участник принимает такие законодательные и иные меры, которые необходимы для квалификации в качестве преступления в соответствии с его внутренним законодательством нарушения правил эксплуатации носителей, предназначенных для хранения, обработки и передачи охраняемой цифровой информации, содержащейся в критической информационной инфраструктуре или информационных системах или информационно-коммуникационных сетях, относящихся к критической информационной инфраструктуре, или нарушения правил доступа к ним, если такое нарушение наносит ущерб критической информационной инфраструктуре. »[110]

Комментарий: Австралия, США, ЕС и его страны-члены, Новая Зеландия, Грузия, Норвегия, Великобритания, Лихтенштейн, Канада, Чили, Япония, Мексика выступают против включения этой статьи в конвенцию и просят ее исключить.

Китай, Иран, Российская Федерация, Венесуэла, Иран, Египет представили:
«Статья 10 тер. Незаконное предоставление услуг.
Каждое государство-участник принимает такие законодательные и другие меры, которые могут потребоваться для квалификации в качестве уголовных преступлений в соответствии с его внутренним законодательством, когда они совершаются умышленно и без права
(a) Предоставление услуг или технической поддержки, включая доступ в Интернет, хостинг серверов, хранение данных в Интернете, передачу сообщений или аналогичные услуги; или
(b) Создание веб-сайтов, коммуникационных сетей

с намерением, чтобы услуга или техническая поддержка использовались для совершения любого из преступлений, признанных таковыми в соответствии с настоящей Конвенцией».[111]

Комментарий: Австралия, США, ЕС и его страны-члены, Новая Зеландия, Грузия, Норвегия, Великобритания, Лихтенштейн, Канада, Япония, Мексика выступают против включения этой статьи в конвенцию и просят ее исключить.

Российская Федерация, Мали, Беларусь, Никарагуа, Буркина-Фасо, Эритрея, Венесуэла, Судан, Куба, Нигерия, Бурунди, КНДР, Египет, Турция, Сьерра-Леоне внесли предложение: «Статья 15 септиес. Преступления, связанные с терроризмом.
Каждое Государство-участник принимает такие законодательные и другие меры, которые могут потребоваться для квалификации в качестве уголовных преступлений, когда они совершаются с помощью информационных и коммуникационных технологий, совершения террористических актов, подстрекательства, вербовки или иного вовлечения в террористическую деятельность, пропаганды и оправдания терроризма или сбора или предоставления средств для его финансирования, подготовка к террористическим актам, содействие связи между террористическими организациями и их членами, включая создание, публикацию или использование сайта, или оказание материально-технической поддержки исполнителям террористических актов, распространение методов изготовления взрывчатых веществ, используемых, в частности, в террористических актах, и распространение раздоров, смуты, ненависти или расизма. «[112]

[110] Тот же источник, стр. 9
[111] Тот же источник, стр. 9
[112] Тот же источник, стр. 19

Комментарий: Канада, США, Новая Зеландия, Доминиканская Республика, Гватемала, Норвегия, Грузия, Австралия, ЕС и его страны-члены, Израиль, Великобритания, Ливан, Лихтенштейн, Чили, Япония, Мексика выступают против включения этой статьи в конвенцию и просят ее исключить.

Алжир, Канада, Российская Федерация предложили сохранить первоначальный текст:
Статья 21. Обвинение, судебное разбирательство и санкции
[...]
«Каждое государство-участник может принимать в соответствии со своим внутренним законодательством такие законодательные и иные меры, которые могут быть необходимы для установления отягчающих обстоятельств в отношении преступлений, признанных таковыми в соответствии со статьями 6-9 настоящей Конвенции, включая обстоятельства, затрагивающие критические информационные инфраструктуры».[113]

Комментарий: Лихтенштейн, Новая Зеландия, Норвегия, Танзания, США, ЕС и его государства-члены, Швейцария, Нигерия, Израиль, Филиппины, Австралия, Грузия, Норвегия, CARICOM выступают против включения этой статьи в конвенцию и просят ее исключить.

«Статья 26. Ускоренное сохранение и частичное раскрытие данных о трафике
Каждое государство-участник принимает в отношении данных о дорожном движении, подлежащих сохранению в соответствии с положениями статьи об ускоренном сохранении хранимых [компьютерных данных] [цифровой информации], такие законодательные и другие меры, которые могут быть необходимы в следующих целях:
[...] (b) Обеспечить оперативное раскрытие компетентному органу государства-участника или лицу, назначенному таким органом, достаточного количества данных о трафике, чтобы государство-участник могло определить поставщиков услуг и путь, по которому было передано сообщение или указанная информация».[114]

«Статья 27. Заказ на производство
Каждое государство-участник принимает такие законодательные и другие меры, которые могут быть необходимы для наделения его компетентных органов полномочиями отдавать распоряжения: [...] (b) Поставщик услуг, предлагающий свои услуги на территории государства-участника, должен представить информацию об абонентах, касающуюся таких услуг, находящуюся во владении или под контролем этого поставщика услуг».[115]

Российская Федерация, Аргентина, Венесуэла, Египет, Южная Африка высказались за сохранение текста следующей статьи:
«Статья 29. Сбор данных о трафике в режиме реального времени[116] 1. Каждое государство-участник принимает такие законодательные и другие меры, которые могут

[113] Тот же источник, стр. 25

[114] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, шестая сессия, 21 августа - 1 сентября 2023 года, проект конвенции (предварительная копия), стр. 13, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/Pre-session-docs/A_AC_291_22_Advance_Copy.pdf

[115] Тот же источник

[116] 1 сентября 2023 года председатель группы АНС обсудил статьи 29 и 30 (сбор данных о трафике в режиме реального времени и перехват данных о контенте соответственно) и сообщил: «Однако в отношении статей

быть необходимы для наделения его компетентных органов полномочиями: (a) собирать или записывать путем применения технических средств на территории этого государства-участника; и (b) принуждать поставщика услуг в рамках имеющихся у него технических возможностей: (i) собирать или регистрировать путем применения технических средств на территории этого Государства-участника; или ii) сотрудничать и оказывать помощь компетентным органам в сборе или регистрации; данных о трафике в режиме реального времени, связанных с определенными сообщениями на его территории, передаваемыми с помощью [компьютерной системы] [устройства информационных и коммуникационных технологий]. 2. Если государство-участник в силу принципов своей внутренней правовой системы не может принять меры, упомянутые в пункте 1 (a), оно может вместо этого принять законодательные и другие меры, которые могут быть необходимы для обеспечения сбора или записи в режиме реального времени данных о трафике, связанных с определенными сообщениями, передаваемыми на его территории, путем применения технических средств на этой территории. 3. Каждое государство-участник принимает такие законодательные и иные меры, которые могут быть необходимы для того, чтобы обязать поставщика услуг сохранять конфиденциальность факта осуществления любого полномочия, предусмотренного в настоящей статье, и любой информации, относящейся к нему».[117]

Комментарий: Сингапур, Швейцария, Малайзия, Вьетнам выступают против включения этой статьи в конвенцию и просят ее исключить.

«Статья 36. Защита персональных данных.
1. Государство-участник, передающее персональные данные в соответствии с настоящей Конвенцией, делает это в соответствии с условиями внутреннего законодательства этого государства-участника и применимого международного права. Государства-участники не обязаны передавать персональные данные в соответствии с настоящей Конвенцией, если они не могут быть предоставлены в соответствии с их действующим законодательством, касающимся защиты персональных данных. Они также могут наложить условия в соответствии с такими применимыми законами, чтобы обеспечить соблюдение требований в ответ на запрос о предоставлении персональных данных. Государствам-участникам рекомендуется заключать двусторонние или многосторонние соглашения для облегчения передачи персональных данных».[118]

CARICOM, ЕС и его государства-члены, Вануату, Новая Зеландия, Албания, Грузия, США, Великобритания, Китай, Норвегия, Кабо Верде, Танзания, Ливан, Колумбия, Эквадор, Пакистан, Швейцария, Тонга, Австралия поддержали включение этого положения в статью 36: «1-бис. Если передача персональных данных не может быть осуществлена в соответствии с пунктом 1, государства-участники могут попытаться наложить соответствующие условия (в соответствии с их применимым законодательством,

29 и 30 несколько делегаций попросили сделать оговорки для посредников, чтобы предложить поправки, и они ожидают дальнейшего обсуждения на 7-й сессии Комитета». Веб-ТВ ООН, (23-е заседание) Шестая сессия Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, 1 сентября 2023 года (начало на отметке 02:01:23), https://media.un.org/en/asset/k17/k17lzfhyyp

[117] Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях, шестая сессия, 21 августа - 1 сентября 2023 года, проект текста конвенции (состояние на 2 сентября 2023 года с обновлениями от государств-членов), стр.33, https://www.unodc.org/documents/Cybercrime/AdHocCommittee/6th_Session/DTC/DTC_rolling_text_02.09.2023.pdf

[118] Тот же источник, стр. 38

касающимся защиты персональных данных [...] для достижения соответствия, чтобы положительно ответить на запрос о предоставлении персональных данных».[119]

Комментарий: Индия предложила исключить вышеуказанное дополнительное положение.

Российская Федерация предложила это дополнение:
«Статья 40. Общие принципы и процедуры, касающиеся взаимной правовой помощи. [...]
3. Взаимная правовая помощь, предоставляемая в соответствии с настоящей статьей, может быть запрошена для любой из следующих целей: [...] [(l-бис) Удаление доменного имени, используемого для преступной деятельности».[120]

«Статья 43. Ускоренное раскрытие сохраненных данных о трафике
1. Если в ходе выполнения просьбы, направленной в соответствии со статьей 42, о сохранении данных о трафике, касающихся конкретного сообщения, запрашиваемое государство-участник обнаруживает, что поставщик услуг в другом государстве-участнике участвовал в передаче сообщения, запрашиваемое государство-участник оперативно раскрывает запрашивающему государству-участнику достаточный объем данных о трафике для идентификации этого поставщика услуг и пути, по которому было передано сообщение».[121]

Статья 45. Взаимная правовая помощь при сборе данных о дорожном движении в режиме реального времени
1. Государства-участники оказывают друг другу взаимную правовую помощь в сборе в режиме реального времени данных о трафике, связанных с определенными сообщениями на их территории, передаваемыми с помощью [компьютерной системы] [устройства информационных и коммуникационных технологий]. С учетом положений пункта 2 такая помощь регулируется условиями и процедурами, предусмотренными внутренним законодательством.»

[...]

«3. В запросе, поданном в соответствии с пунктом 1 настоящей статьи, должны быть указаны: (c) [компьютерные данные] [цифровая информация], в отношении которых требуется сбор данных о трафике, и их связь с правонарушением или другим противоправным деянием; d) любые имеющиеся данные, позволяющие установить владельца или пользователя данных или местонахождение [компьютерной системы] [устройства информационных и коммуникационных технологий];».[122]

Контекст. АНС проводит неофициальные консультации в межсессионный период между 6-й и последней сессиями в январе–феврале 2024 года. Многосторонние заинтересованные стороны не были приглашены на эти консультации, они предназначены только для правительств. Цель председателя — подготовить сокращенный «чистый» проект текста Конвенции к концу ноября 2023 года.

[119] Тот же источник
[120] Тот же источник, стр. 47
[121] Государства-участники согласились с этим положением «до последующего утверждения», тот же источник, стр. 26
[122] Тот же источник

Глобальный цифровой договор и Саммит будущего

Введение/История вопроса

В 2020 году в докладе Генерального секретаря Гутерриша «Наша общая повестка дня» было предложено провести Саммит будущего с технологическим треком, ведущим к Глобальному цифровому договору (GDC): Кроме того, опираясь на рекомендации «дорожной карты» по цифровому сотрудничеству (см. A/74/821), Организация Объединенных Наций, правительства, частный сектор и гражданское общество могли бы объединиться в рамках многостороннего трека цифровых технологий в рамках подготовки к Саммиту будущего для согласования Глобального цифрового договора. В нем будут изложены общие принципы открытого, свободного и безопасного цифрового будущего для всех».[123]

Глобальный цифровой договор

25 апреля 2023 года Генеральный секретарь ООН опубликовал аналитическую записку № 5, в которой, в частности, содержалась формулировка Генерального секретаря ООН о параметрах концепции будущего GDC. См. блог ICANN, где некоторые цитаты из GDC рассматриваются в контексте.[124]

Выдержки из письменных материалов, представленных в GDC государствами-членами, коалициями и наднациональными организациями

Контекст. Офис Посланника ООН по технологиям весной и летом 2023 года организовал серию подробных обзоров по вопросам, связанным с GDC. Персонал GE ICANN присутствовал на этих презентациях, однако обсуждения официально не записывались, и GE не может предоставить цитаты из этих дискуссий. Однако некоторые из письменных материалов отражают устные выступления делегаций стран в ходе этих обсуждений.

Апрель 2023 года

13 апреля 2023 года Европейский Союз заявил: «ЕС считает, что [...] интернет должен оставаться открытым, глобальным, свободным, функционально совместимым и децентрализованным. Мы решительно поддерживаем мультистейкхолдерный подход к управлению интернетом, который гарантирует, что все участники, включая правительства, частный сектор, гражданское общество и технические сообщества,

[123] Декларация о праздновании семьдесят пятой годовщины Организации Объединенных Наций, Резолюция, принятая Генеральной Ассамблеей 21 сентября 2020 года, A/RES/75/1, 28 сентября 2020 года, https://documents.un.org/prod/ods.nsf/xpSearchResultsE.xsp

[124] Блоги ICANN, 13 июня 2023 года, https://www.icann.org/ru/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-ru

участвуют в формировании будущего интернета».
[…]
«Положительным примером дальнейшего развития подхода с участием многих заинтересованных сторон стала успешная передача координирующей роли в исполнении функций IANA к ICANN в 2016 году. Все заинтересованные стороны, включая правительства, могут принять участие в работе ICANN и помочь повысить безопасность и стабильность глобальной системы доменных имен DNS».[125]

Исламская Республика Иран заявила: «Подготовка концепции эффективного сотрудничества между хранителями экосистемы управления интернетом, а также хранителями IP и системы управления и правоохранительными и судебными органами стран в области предотвращения и борьбы с киберпреступностью».[126]

Нидерланды заявили: «Глобальный цифровой договор должен взять на себя обязательство не допускать фрагментации технической инфраструктуры интернета, препятствующей способности систем к взаимодействию и угрожающей общей целостности и доступности основной инфраструктуры интернета. Сюда входят маршрутизация и пересылка пакетов, системы именования и нумерации, технологии шифрования и базовые физические инфраструктуры».[127]

G77 и Китай заявили: «Глобальный цифровой договор должен опираться на ключевые документы и форумы по развитию цифрового сотрудничества, в частности, Всемирную встречу на высшем уровне по вопросам информационного общества (ВВУИО), в частности Тунисскую программу и Женевский план действий, Форум по управлению интернетом, а также учитывать Дорожную карту цифрового сотрудничества, представленную Генеральным секретарем».
[…]
«Группа подчеркивает, что результаты ВВУИО должны быть сохранены в качестве руководства для международного цифрового сотрудничества и управления интернетом, поскольку они основаны на принципах, благоприятствующих развитию».
«Тунисская программа и Женевская декларация принципов и плана действий должны стать руководящими принципами для разработки любого нового механизма цифрового сотрудничества, включая GDC».

[...]
«Мы признаем, что ни одной стране или заинтересованному лицу, или их небольшой группе, не должно быть позволено монополизировать или контролировать основную инфраструктуру интернета».
«Государства, обладающие монополией и доминирующим положением в сфере ИКТ, включая интернет, не должны использовать достижения ИКТ в качестве инструментов

[125] Делегация Европейского Союза при Организации Объединенных Наций в Нью-Йорке, Заявление ЕС — Глобальный цифровой договор: Всесторонний анализ управления интернетом, 13 апреля 2023 года, https://www.eeas.europa.eu/delegations/un-new-york/eu-statement-global-digital-compact-deep-dive-internet-governance_en?s=63
[126] Предложение Исламской Республики Иран по Глобальному цифровому договору, апрель 2023 года, последнее изменение 2 мая 2023 года, стр. 20, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_Islamic-Republic-Iran.pdf
[127] Глобальный цифровой договор, представленный Королевством Нидерландов, 28 апреля 2023 года, стр. 7, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission-Kingdom-of-the-Netherlands.pdf

сдерживания и подавления законного экономического и технологического развития других государств».
«Глобальный цифровой договор должен подтвердить, что интернет должен быть открытым, безопасным, инклюзивным, доступным и функционально совместимым».
[...]
«Вопросы управления интернетом должны решаться в рамках глобальной структуры, опирающейся на систему ООН, при широком участии всех государств с применением подхода, основанного на участии многих заинтересованных сторон, как это было предусмотрено в итоговых документах ВВУИО».
[…]
«Необходимо поддерживать безопасность, надежность и стабильность интернета, не ставя под угрозу усилия по достижению устойчивого развития. Международное сотрудничество через укрепление многосторонних отношений в этой области очень важно».[128]

Сальвадор подтвердил «… важность продолжения применения подхода с участием многих заинтересованных сторон, изложенного в Женевском саммите 2003 года и Тунисской программе 2005 года».[129]

Франция пишет: **«**Предлагаемые действия: […] Также необходимо будет поработать над протоколами, чтобы сохранить единство, нейтральность и отказоустойчивость интернета».[130]

Китайская Народная Республика заявила: «Государства имеют право участвовать в управлении и распределении основных международных интернет-ресурсов на равных условиях и должны воздерживаться от использования интернет-ресурсов и технологий для подрыва законных прав других государств на доступ к интернету, что ставит под угрозу безопасность, стабильность и связность глобального интернета».[131]
[...]
«Государства должны способствовать формированию киберпространства, характеризующегося миром, безопасностью, открытостью, сотрудничеством и порядком, и выступать против разделения и фрагментации интернета. Государства должны сформулировать глобальные функционально совместимые общие правила и стандарты в киберпространстве при широком участии государств-членов под эгидой ООН и сохранять приверженность созданию международной системы управления интернетом, характеризующейся многосторонностью, демократией и транспарентностью».[132]

---

[128] Предложения G77 и Китая для обсуждения Глобального цифрового договора, 28 апреля 2023 г, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_G77-and-China.pdf
[129] Предложение Сальвадора по представленным тематическим областям Глобального цифрового договора, последнее изменение 1 мая 2023 года, стр.3, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_El-Salvador.pdf
[130] Предложение Франции по Глобальному цифровому договору — неофициальный перевод, последнее изменение 8 мая 2023 года, стр. 5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_France.pdf
[131] Позиция Китая по вопросам глобального цифрового управления (предложение по Глобальному цифровому договору), последнее изменение 24 мая 2023 г., стр. 5, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/GDC-submission_China.pdf
[132] Тот же источник, стр. 13

Неформальная встреча, посвященная выходу аналитической записки «Наша общая повестка дня» № 5 Глобальный цифровой договор — открытое, свободное и безопасное цифровое будущее для всех[133]

На неофициальной встрече в штаб-квартире ООН 5 июня 2023 года Генеральный секретарь Антониу Гутерриш представил аналитическую записку № 5. В своем вступительном слове г-н Гутерриш сказал: «В документе предлагается провести Форум цифрового сотрудничества, который оценит прогресс в области цифрового управления и выявит недостатки. Это будет первая глобальная структура, объединяющая все заинтересованные стороны для согласованных действий в области цифровых технологий. Он будет сотрудничать с региональными органами и сетями многих заинтересованных сторон, а также поддерживать обмен между существующими органами, такими как Форум по управлению интернетом. В нем будут принимать участие широкие слои населения, привлекать тех, кто разрабатывает цифровые технологии, чтобы понять их потенциал и способствовать их ответственному применению».[134]

Отклики делегатов некоторых стран-членов ООН:

Европейский Союз (от имени 27 государств): «Поддержка и укрепление уже существующих структур, таких как Форум по управлению интернетом, МСЭ, ЮНЕСКО и другие, может помочь избежать дублирования и фрагментации усилий». […] «Мультистейкхолдерный подход будет иметь ключевое значение для поддержки GDC».[135]

Канада (также от имени Австралии и Новой Зеландии, или CANZ): «Наши страны полностью привержены сотрудничеству с другими странами, чтобы обеспечить продолжение существования свободного, открытого, функционально совместимого, надежного и безопасного интернета во всем мире». […] Мы также являемся убежденными сторонниками мультистейкхолдерной модели управления интернетом, которая является основой открытости, отказоустойчивости и стабильности интернета. Мультистейкхолдерный подход признает, что все заинтересованы в том, как управляется интернет. Мы должны признать ту роль, которую существующие организации с участием многих заинтересованных сторон успешно играют в развитии и функционировании интернета. Мы восхищаемся амбициозностью предложений, содержащихся в аналитической записке, однако мы настоятельно призываем к тому, чтобы любые потенциальные новые инициативы в первую очередь были направлены на укрепление и дополнение существующих успешных усилий в области глобального цифрового сотрудничества в ООН».[136]

---

[133] Подробную информацию о документе можно найти на странице «Блоги ICANN»: https://www.icann.org/ru/blogs/details/un-secretary-general-policy-report-considerations-for-the-icann-community-13-06-2023-ru

[134] Брифинг Генерального секретаря по поводу представления серии документов «Наша общая повестка дня», Брифинг Генерального секретаря «Наша общая повестка дня» для Саммита будущего (организованный Канцелярией Генерального секретаря (EOSG), Веб-ТВ ООН, 7 мая 2023 года (начало на отметке 19:35), https://media.un.org/en/asset/k1n/k1nugz7a7n,

[135] Тот же источник, (начало на отметке 20:30)

[136] Тот же источник (начало на отметке 30:33)

Литва: «Я бы особенно хотел подчеркнуть важность привлечения специализированных учреждений, таких как МСЭ, путем предоставления им более четко определенной роли в содействии достижению целей Договора».[137]

Пакистан: «Мы бы хотели, чтобы межправительственный процесс направил договор в сторону развития, а не регулирования, и это должно соответствовать Тунисской программе, в которой государственная политика, связанная с интернетом, является компетенцией, суверенным правом государств. Конечно, мы также рассматриваем этот Форум цифрового сотрудничества, который мы хотели бы видеть, как он будет взаимодействовать с Форумом по управлению интернетом и Форумом ВВУИО, а также с Рабочей группой открытого состава по безопасности использования ИКТ».[138]

Соединенные Штаты Америки: «В связи с тем, что Глобальный цифровой договор должен обеспечить транспарентность, инклюзивность и активное и значимое участие всех заинтересованных сторон в процессе GDC, мы призываем ООН предоставить заинтересованному сообществу возможность высказать свое мнение по аналитической записке GDC».[139] «Попытки направить цифровое сотрудничество из Нью-Йорка не отражают того факта, что мультистейкхолдерные, многосекторальные и децентрализованные подходы предлагают более эффективные средства использования цифровых технологий для достижения ЦУР».[140]

Швейцария: «Предложение о создании нового Форума цифрового сотрудничества рискует неоправданно обременить реализацию Договора. Вместо того чтобы принести реальную пользу, он грозит дублированием усилий, уже предпринятых в рамках цифровых структур для существующего сотрудничества. В частности, Форум по управлению интернетом продемонстрировал свою эффективность в последующей работе с участием многих заинтересованных сторон по вопросам, охватываемым Договором».[141]

Эстония: «Для достижения универсальной и значимой связности нам необходимо многостороннее сотрудничество, которое опирается на наши общие ценности и общие принципы, как мы уже договорились в Тунисской программе».[142]

Китай: «Касательно GDC. Китай поддерживает Организацию Объединенных Наций в том, что она играет ключевую роль в координации совместных усилий различных заинтересованных сторон по укреплению цифрового сотрудничества, сокращению цифрового разрыва и совершенствованию цифрового управления, чтобы цифровые технологии могли принести пользу всему человечеству. Процесс разработки должен быть ориентирован на решение конкретных вопросов...».[143]

Индонезия: "Что касается GDC, мы отмечаем, что GDC разделяет схожие идеи с темой Форума по управлению Интернетом 2023 года. И в этой связи мы хотели бы услышать мнения о том, как сделать так, чтобы GDC, в частности инициатива Глобального форума

[137] Тот же источник (начало на отметке 34:00)
[138] Тот же источник (начало на отметке 39:38)
[139] Тот же источник, (начало на отметке 01:06)
[140] Тот же источник, (начало на отметке 01:08)
[141] Тот же источник, (начало на отметке 01:10)
[142] Тот же источник, (начало на отметке 01:12)
[143] Тот же источник, (начало на отметке 01:18)

цифрового сотрудничества, дополняла существующий процесс, избегала дублирования и укрепляла IGF?»[144]

Великобритания: «Любая новая инициатива должна дополнять существующие усилия по цифровому сотрудничеству, которые уже предпринимаются в ООН. Великобритания признает, что существующие организации с участием многих заинтересованных сторон являются составными частями открытого, отказоустойчивого и стабильного Интернета».[145]

Индия: «Наш подход должен быть основан на недопущении дублирования усилий или создания параллельных процессов».[146]

В своем заключительном слове Генеральный секретарь ООН сказал: «Но мы должны различать, каковы рамки межправительственного процесса, поскольку он связан с суверенитетом государств-членов, и каковы рамки, области, в которых лучше держать всех вовлеченными, чтобы попытаться заставить все двигаться в позитивном направлении». […] Я ожидал вопроса о форуме[147], потому что мы также проводим обсуждения в наших командах. Это не вопрос веры. Это то, что мы предлагаем, если государства-члены согласятся — хорошо, если нет — ничего страшного не случится. Но, как бы то ни было, я считаю, что вопрос не в дублировании. Вопрос в том, где все сходится. Потому что у нас есть несколько вещей. У нас есть Форум по управлению Интернетом, у нас есть механизмы МСЭ, у нас есть механизмы ЮНЕСКО, но они разделены. И я считаю, что нам нужно что-то здесь, в Нью-Йорке, рядом с Генеральной Ассамблеей, что позволит объединить все эти вещи. […] Это не логика дублирования, это логика гарантии того, что есть место, где все эти вещи можно увидеть вместе. И это единственная причина, по которой это предложение было вынесено на обсуждение».[148]

Совещание министров по подготовке Саммита будущего — Генеральная Ассамблея, 78-я сессия

21 сентября 2023 года был сделан ряд заявлений на уровне министров и на высоком уровне по вопросам Глобального цифрового договора и управления интернетом, в том числе:

Руанда: «Глобальное цифровое сотрудничество будет ключевым в рамках GDC [, оно] обеспечивает такую концепцию цифрового сотрудничества».[149]

[144] Тот же источник, (начало на отметке 01:19)
[145] Тот же источник, (начало на отметке 01:24)
[146] Тот же источник, (начало на отметке 01:34)
[147] здесь - Форум цифрового сотрудничества
[148] Брифинг Генерального секретаря по поводу представления серии документов «Наша общая повестка дня», Брифинг Генерального секретаря «Наша общая повестка дня» для Саммита будущего (организованный Канцелярией Генерального секретаря (EOSG), Веб-ТВ ООН, 7 мая 2023 года (начало на отметке 01:55), https://media.un.org/en/asset/k1n/k1nugz7a7n,
[149] Веб-ТВ ООН, (открытие, пленарное заседание, закрытие) заседание министров по подготовке Саммита будущего — Генеральная Ассамблея, 78-я сессия, 21 сентября 2023 года, (начало на отметке: 42:52), https://media.un.org/en/asset/k1z/k1zzbbnqaq

Норвегия: «Мы также должны вместе работать над справедливой глобальной цифровой трансформацией и Глобальным цифровым договором».[150]

Россия: «Мы поддерживаем включение вопросов технологий и инноваций в повестку дня саммита, для преодоления цифрового неравенства и демократизации управления интернетом и регулирования ИИ при строгом соблюдении национального суверенитета всех государств».[151]

Болгария: «Сохранение мультистейкхолдерного подхода и целостности интернета — вот где мы должны добиться наилучших результатов».[152]

Мексика: «Мы полностью поддерживаем Глобальный цифровой договор».[153]

МСЭ: «Эти проблемы требуют совместной работы всех заинтересованных сторон. Всемирная встреча на высшем уровне по вопросам информационного общества и последующие процессы, такие как IGF и Форум ВВУИО, должны сыграть важную роль, и это было признано сокоординаторами Глобального цифрового договора».[154]

Индия: «Мы приветствуем цель SoTF — реализовать Глобальный цифровой договор, чтобы свести к минимуму любое цифровое неравенство».[155]

Зимбабве: «Нам необходим более целостный многосторонний подход к технологическому управлению с учетом стремительного развития технологий и связанных с ними угроз и рисков. Нам срочно нужен Глобальный цифровой договор».[156]

Финляндия: «Одним из ключевых направлений будущего саммита станет согласование Глобального цифрового договора. Договор должен принести реальную и ощутимую пользу в том, как мы сотрудничаем по общим цифровым приоритетам, стимулируем решения в интересах ЦУР и защищаем права человека в цифровом пространстве, включая неприкосновенность частной жизни и свободу выражения мнений».[157]

Другие инициативы ООН

Официальные документы 77-й сессии Генеральной Ассамблеи ООН.

15 мая 2023 года Россия, Беларусь, Северная Корея, Никарагуа и Сирия (в качестве соавторов) представили концепцию Конвенции ООН об обеспечении международной

[150] Тот же источник (начало на отметке: 1:39:10)
[151] Тот же источник (начало на отметке: 2:55:05)
[152] Тот же источник, см. оригинал на французском языке (начало на отметке: 3:24:40)
[153] Тот же источник (начало на отметке: 4:05:19)
[154] Тот же источник (начало на отметке: 5:15:40)
[155] Тот же источник (начало на отметке: 6:36:55)
[156] Тот же источник (начало на отметке: 7:10:40)
[157] Тот же источник (начало на отметке: 7:48:55)

информационной безопасности как официальный документ 77-й сессии Генеральной Ассамблеи ООН.[158]
Среди прочего, соавторы назвали следующий принцип и предложение, которые «могли бы послужить основой для положений Конвенции, регулирующих деятельность государств и определяющих права и обязанности государств в отношении содействия укреплению государственного потенциала в области безопасности при использовании информационных и коммуникационных технологий»: [...] содействие развитию и использованию безопасных информационных и коммуникационных технологий в соответствии с принципом нейтральности глобальной коммуникационной сети, включая эволюционное реформирование протоколов и методов передачи информации для исключения возможности использования этой сети в преступных целях;»[159]

Контекст. Россия и соавторы проекта конвенции настаивали на том, чтобы концепция проекта конвенции была упомянута в ежегодном отчете о ходе работы РГОС за 2023 год. Россия заявила, что Китай и Иран также поддерживают включение упоминания о проекте конвенции в ежегодный отчет о ходе работы РГОС.[160]

Заявления Посланника Генерального секретаря по технологиям

13 октября 2022 года Посланник ООН по технологиям Амандип Сингх Гилл сказал: «Саммит будущего в 2024 году — это возможность для международного сообщества перезагрузить многосторонний подход и лучше подготовиться к вызовам завтрашнего дня.

Решение о проведении саммита было принято Генеральной Ассамблеей ООН на основании доклада, представить который попросили Генерального секретаря ООН. Этот доклад называется «Наша общая повестка дня», и Глобальный цифровой договор (GDC) является одним из предложений, содержащихся в этом докладе. Он должен быть принят на Саммите будущего».[161]
24 октября 2022 года представитель Гилл сказал: «Я без колебаний могу сказать, что приверженность мультистейкхолдерным подходам очень сильна. На самом деле, когда Генеральный секретарь выступал перед Генеральной Ассамблеей, он ясно дал понять, что либо мы придем к GDC через процесс с участием многих заинтересованных сторон, либо не придем вообще. Это было очень четкое, очень сильное заявление, сделанное в Нью-Йорке. И мы выполняем это обязательство, например, через эти консультации и многие другие, через активное взаимодействие не только с IGF, но и с другими форумами, в том числе с ICANN».[162] Он продолжил: «теперь ваш вопрос о том, как мы можем выйти за рамки ритуала [к] сути многосторонних подходов и как мы можем решить эту проблему, которая заключается в том, что либо это межправительственная

[158] Министерство иностранных дел Российской Федерации, пресс-релиз о концепции Конвенции ООН об обеспечении международной информационной безопасности, 16 мая 2023 года, https://mid.ru/ru/foreign_policy/news/1870609/?lang=en
[159] Обновленная концепция Конвенция ООН об обеспечении международной информационной безопасности, 15 мая 2023 года, стр. 8, https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_Russian__Federation.pdf
[160] Веб-ТВ ООН, Рабочая группа открытого состава по информационных и коммуникационных технологий (ICT) (8-е заседание) — пятая основная сессия, 27 июля 2023 года (начало на отметке 13:50), https://media.un.org/en/asset/k1n/k1ngmoogyi
[161] Новости МСЭ, Создание Глобального цифрового договора: вопросы и ответы с Амандипом Сингхом Гиллом, 13 октября 2023 года, https://www.itu.int/hub/2022/10/establishing-the-global-digital-compact-qa-with-amandeep-singh-gill/
[162] IGF, Встреча в ратуше с Посланником Генерального секретаря ООН по технологиям, 24 октября 2022 года (начало на отметке 49:53), https://youtu.be/NEmXNzQzsCk?t=2991

многосторонность, либо это мультистейкхолдерные подходы, которые в конечном итоге являются консультативными интересными обсуждениями, но каков путь к реализации? Мы пытаемся справиться с этой проблемой, но, честно говоря, никто не смог ее решить».[163]
«Я слышал в Нью-Йорке, что тунисская формула ВВУИО — это хорошая формула для участия многих заинтересованных сторон. Вы знаете, что эта формулировка входит в наши соответствующие мандаты и полномочия. У меня нет перед глазами точной формулировки, но для одних эта формула не заходит достаточно далеко, для других — слишком далеко. Посмотрим, что получится в итоге — это тоже один из хороших примеров, на который стоит обратить внимание. Я упомянул два недавних опыта, относительно позитивных: обсуждение киберпреступности и обсуждение в МСЭ. Так что, возможно, мы сможем выработать *уникальную* формулу, которая удовлетворяет Дэвида, Адама[164] и всех остальных в этом плане».[165]

23 июня 2023 года Посланник ООН по технологиям сказал: «Я хотел бы предложить вам ознакомиться с последним разделом этой аналитической записки [UNSecGen], посвященным идее регулярной оценки выполнения договора, чтобы идти в ногу с развитием технологий. И единственное, что я хочу еще раз подчеркнуть, особенно ссылаясь на предыдущие выступления на этой совещании, — это то, что это форум с участием многих заинтересованных сторон. Итак, подготовка — трехсторонняя, эти слова четко используются во всем гражданском обществе, которое включает всех членов технического сообщества, сектор науки и образования, и ценность научных, независимых научных экспертных знаний, в частности, связанных с искусственным интеллектом, в этом отношении сегодня есть четкое понимание, есть частный сектор и есть правительства».[166]

Сопутствующее мероприятие Недели борьбы с терроризмом 2023

22 июня 2023 года в рамках инициативы «Техника против терроризма», поддержанной Исполнительным директоратом ООН по борьбе с терроризмом (UN CTED) призвал государства «рассмотреть пути совершенствования механизмов удаления сайтов, поддерживаемых террористами, в том числе помочь нам вмешаться в работу регистраторов доменных имен, сетей распространения контента и хостинг-провайдеров».[167]

---

[163] Тот же источник (начало на отметке 51:31), https://youtu.be/NEmXNzQzsCk?t=3091
[164] Здесь Посланник ООН по технологиям ссылается на вопросы, заданные ему представителем Канады и членом MAG о роли процесса ВВУИО и технического сообщества.
[165] Тот же источник, (начало на отметке 1:06:13), https://youtu.be/NEmXNzQzsCk?t=3973
[166] Видео на YouTube, EuroDIG 2023 — подготовка 05 | Давайте продвигать европейское видение цифрового управления и сотрудничества, 23 июня 2023 года, (начало на отметке 1:36:42), https://youtu.be/RctcgFscohU?t=5802
[167] Веб-ТВ ООН, Предотвращение и противодействие использованию новых и новейших технологий в террористических целях: путь вперед для целостного многостороннего ответа (сопутствующее мероприятие в рамках Недели борьбы с терроризмом 2023 года), 22 июня 2023 года (начало на отметке 1:08:27), https://media.un.org/en/asset/k1i/k1iy7ltzvt

Заключение

Текущие обсуждения в ООН в формате РГОС завершатся в 2025 году, и отчет станет итогом этих обсуждений, если он будет принят в результате консенсуса. Планируется, что работа АНС завершится в феврале 2024 года принятием конвенции о киберпреступности на основе консенсуса или, если консенсус не будет достигнут, большинством в две трети голосов делегаций стран, участвующих в голосовании и присутствующих на заседании. GE будет следить за обоими процессами и отчитываться о них, хотя считает, что их результаты, скорее всего, окажут нулевое или минимальное влияние на миссию ICANN.

Переговоры по GDC начнутся в январе 2024 года, а заключительный этап планируется провести 20-23 сентября 2024 года во время Саммита будущего, где, как ожидается, Договор будет принят на основе консенсуса. В настоящее время этот процесс представляет для организации слишком много неизвестных. GE будет следить за всеми обсуждениями в GDC и сообщать сообществу ICANN о ходе и развитии событий по мере того, как будут разворачиваться переговоры.

Один мир, один Интернет

Заходите к нам на **icann.org**

@icann

facebook.com/icannorg

youtube.com/icannnews

flickr.com/icann

linkedin.com/company/icann

soundcloud.com/icann

instagram.com/icannorg