Новости ООН: обсуждение вопросов, связанных с киберпространством

Взаимодействие ICANN с правительственными и межправительственными организациями (МПО)

Вени Марковски (Veni Markovski)
GE-005
15 июля 2020 г.

ICANN

СОДЕРЖАНИЕ

Предисловие **3**
Отчеты о деятельности ОЕСЕ, РГОС и ГПЭ **4**
ОЕСЕ 4
РГОС 4
Группа правительственных экспертов (ГПЭ) 9
Участие ICANN и дальнейшие действия **9**
ПРИЛОЖЕНИЕ 1 **10**
Справочная информация о комитетах ООН и ГА ООН 10

Предисловие

В настоящем документе представлена свежая информация о деятельности рабочих групп Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН), которые обсуждают вопросы, связанные с интернетом и кибербезопасностью.

Во время этих обсуждений периодически поднимаются вопросы, касающиеся миссии ICANN, что может происходить и в будущем. Мониторинг таких дискуссий является частью работы отдела взаимодействия с правительствами (GE) корпорации ICANN, которая направлена на поддержку выполнения миссии ICANN, а также демонстрирует стремление и обязанность GE информировать все сообщество ICANN о вопросах, представляющих важность для глобального единого функционально совместимого интернета и его системы уникальных идентификаторов.[1]

В нашем предыдущем документе «Краткий обзор обсуждений кибербезопасности и киберпреступности в ООН» рассказывалось о создании различных рабочих групп и процессов в Организации Объединенных Наций (ООН).[2]В этом документе мы уделяем основное внимание отчету о деятельности Рабочей группы открытого состава (РГОС) и Специального межправительственного комитета экспертов открытого состава (ОЕСЕ).

[1] Как указано в нашем пятилетнем операционном и финансовом плане, стр. 47:«Мониторинг законодательства, правил, норм, принципов и инициатив, которые могут повлиять на миссию ICANN»
[2]Данный документ входит в состав серии, публикуемой отделом взаимодействия с правительствами, начиная с 28 февраля 2020 года. Со всеми документами по взаимодействию с правительствами можно ознакомиться на этой веб-станице нашего сайта.

Отчеты о деятельности ОЕСЕ, РГОС и ГПЭ

ОЕСЕ

Группа ОЕСЕ[3] начала свою работу по «борьбе с использованием информационных и коммуникационных технологий в преступных целях» с опубликования документа, который содержит предлагаемые основные принципы и методы на следующие четыре года.[4] В этом документе, который планируется обсудить на первом совещании группы в августе 2020 года, изложена концепция работы ОЕСЕ до ее завершения в июне 2024 года.

10 июля состоялась виртуальная неофициальная встреча, посвященная организационной сессии Специального комитета по киберпреступности. На этой встрече Управление ООН по наркотикам и преступности (ЮНОДК) представило обновленную информацию по процедурным вопросам, связанным с августовской организационной сессией Специального комитета, а затем государства-члены обсудили предварительную повестку дня этой организационной сессии.[5] Более подробная информация об этом июльском виртуальном неофициальном совещании представлена на сайте ОЕСЕ, в частности в документе под названием «Резюме информации, представленной директором отдела по вопросам международных договоров ЮНОДК на неофициальной встрече 10 июля 2020 года».[6]

По состоянию на 13 июля 2020 года ОЕСЕ опубликовал на своей веб-странице комментарии следующих государств-членов: Австралия, Канада, Доминиканская Республика, Европейский Союз, Исламская Республика Иран, Япония, Российская Федерация, Соединенное Королевство Великобритании и Северной Ирландии и Соединенные Штаты Америки.

РГОС

За период с марта 2020 года. 11 марта 2020 года председатель РГОС[7] опубликовал предварительный проект отчета.[8] Этот документ было предложено прокомментировать всем заинтересованным сторонам и обсудить на личной встрече в конце марта 2020 года. Однако из-за COVID-19 эта встреча не состоялась.[9] Вместо этого государствам-членам

[3] ОЕСЕ — это Специальный межправительственный комитет экспертов открытого состава, в состав которого входят представители всех государств-членов ООН, и ему поручено разработать новую конвенцию ООН о киберпреступности. В настоящем документе используется термин «конвенция о киберпреступности», однако ООН использует термин «всеобщая международная конвенция о борьбе с использованием информационно-коммуникационных технологий в преступных целях».
[4] Документ опубликован здесь.
[5] Управление ООН по наркотикам и преступности, https://www.unodc.org/
[6] Загрузить PDF-файл можно здесь.
[7] РГОС — это Рабочая группа открытого состава по вопросам достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности; в своем документе мы используем термин «кибербезопасность».
[8] Загрузить PDF-файл можно здесь.
[9] Примечание: COVID-19 нарушил обычный режим работы ООН и вышеупомянутых рабочих групп. Например, РГОС провела первый раунд своих виртуальных неофициальных совещаний в июне и июле 2020 года.

было предложено отправить письменные комментарии. Десятки государств-членов, межправительственных организаций и неправительственных организаций прислали свои комментарии, которые были опубликованы на сайте группы.[10]

В этом документе мы цитируем некоторые комментарии, представленные в ответ на просьбу председателя прокомментировать документ.[11] Мы обращаем внимание только на те комментарии, которые могут затрагивать миссию или сферу компетенции ICANN.

***

Пункт 38 предварительного проекта отчета начинается так:

«*Государства в ходе обсуждения и путем отправки письменных комментариев также выдвигали предложения по «совершенствованию» и дальнейшему уточнению норм. В частности, поступили следующие предложения: государства должны подтвердить свою приверженность международному миру и безопасности при использовании ИКТ; необходимо вновь заявить, что государства несут основную ответственность за сохранение безопасной, надежной и надежной среды ИКТ; необходимо защитить общедоступность и целостность публичного ядра интернета; [...вырезано...]».*

Комментарии некоторых государств-членов (в алфавитном порядке) к предварительному проекту отчета

> Бразилия:«*По мнению Бразилии, ИТ-инфраструктуры, лежащие в основе проведения избирательных процессов, заслуживают такого же уровня защиты, что и публичное ядро интернета (пункт 38)».*
>
> Китай:*«Учитывая, что у нас ограниченное количество времени, следует избегать включения в отчет понятий, относительно которых еще не достигнут глобальный консенсус (таких как «публичное ядро»)».*
> и: *«На предыдущих двух сессиях стороны, в том числе Китай, выдвинули десятки конструктивных предложений по таким вопросам, как киберсуверенитет, безопасность цепочки поставок, защита критически важной инфраструктуры, отказ от односторонних санкций и борьба с кибертерроризмом. Надеемся, что эти предложения могут быть включены в отчет».*
>
> Египет: «*Следует рекомендовать государствам-членам выработать согласованное общее определение того, что представляет собой «критически важная инфраструктура», чтобы в установленном порядке договориться о запрещении любого действия, при котором наступательный потенциал ИКТ сознательно или преднамеренно используется для повреждения или нанесения иного ущерба использованию и эксплуатации критически важной инфраструктуры*».
>
> Германия: *«Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности публичного*

[10] https://www.un.org/disarmament/open-ended-working-group/
[11] См. приглашение здесь.

ядра интернета и, следовательно, стабильности киберпространства». Это [стало бы] руководством по реализации рекомендации 13(f) ГПЭ ООН 2015 года и, соответственно, также относилось бы к области действия рекомендации 13(g) ГПЭ ООН 2015 года
и: *«Что касается пункта 31, Германия хотела бы подчеркнуть, что основное внимание РГОС должно быть направлено на укрепление существующих норм и улучшение их понимания и реализации. В этой связи мы считаем предложения защитить публичное ядро интернета, предотвратить нарушение работы инфраструктуры, необходимой для политических процессов, не наносить ущерб медицинским учреждениям и сделать акцент на транснациональной инфраструктуре полезными дополнениями к уже существующим нормам защиты критически важной инфраструктуры, как указано в отчете ГПЭ за 2015 год».*

Иран: *«Однако в предварительном проекте не признаются некоторые важные соответствующие угрозы, включая односторонние принудительные меры, монополию в области управления интернетом, анонимность людей и вещей, агрессивные стратегии и политику действий в киберпространстве и так далее, которые несомненно влияют на информированность, стабильность и возможности стран».*

Нидерланды: *«Для устранения этих угроз Нидерланды хотели бы предложить РГОС считать рекомендацию, что «Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности публичного ядра интернета и, следовательно, стабильности киберпространства» руководством по реализации рекомендации 13(f) ГПЭ ООН 2015 года и, соответственно, также относящейся к области действия рекомендации 13(g) ГПЭ ООН 2015 года».*
и: *«Нидерланды хотели бы предложить РГОС рассмотреть в своем отчете угрозу, которую операции в киберпространстве создают для общедоступности или целостности публичного ядра интернета. С течением лет операции в киберпространстве, направленные на нарушение целостности, функционирования и доступности интернета, стали реальной и значимой угрозой».*

Никарагуа: отмечает, что нынешнее *«недостаточное регулирование деятельности частного сектора в области ИКТ»* создает *«большую угрозу для развития среды мирного использования ИКТ».*

Пакистан: *«Следует рекомендовать государствам-членам выработать согласованное общее определение того, что представляет собой «критически важная инфраструктура», чтобы договориться о запрете деятельности в сфере ИКТ, направленной на сознательное или умышленное повреждение или иной ущерб использованию и эксплуатации критически важной инфраструктуры».*

Россия: *«Важность «подхода с участием многих заинтересованных сторон» с акцентом на вклад негосударственного сектора, бизнеса и сектора науки и образования в обеспечение ответственного поведения в информационном пространстве искусственно преувеличена. В то же время проблема недостаточного регулирования деятельности частного сектора в*

сфере ИКТ и все более актуальная проблема монополизации этой области упускается из виду как одна из ключевых угроз для развития мирной и конкурентной среды ИКТ».

Швейцария: *«Например, предложения, касающиеся защиты публичного ядра интернета, предотвращения ущерба медицинским учреждениям, нарушения работы инфраструктуры, необходимой для политических процессов, и соответствующей критически важной транснациональной инфраструктуры, по нашему мнению, могли бы стать ценными принципами реализации существующих норм».*

США: *«...выборочное уточнение норм или выявление конкретных критически важных секторов инфраструктуры сопряжено с определенным риском того, что некоторые вопросы получат приоритет перед другими».*

Европейский Союз: *«Таким образом, защита критически важной инфраструктуры интернета настолько важна, что ЕС и его государства-члены хотели бы предложить РГОС рассмотреть в своем отчете эти угрозы, в том числе угрозу для общедоступности или целостности публичного ядра интернета».*

Комментарии неправительственных организаций

Global Partners Digital: *«Рекомендация: Мы поддерживаем рекомендации Нидерландов, содержащиеся в «неофициальном документе», в отношении уточнения и предоставления дополнительных указаний по нормам (f) и (g) в отчете ГПЭ ООН 2015 года (рез. 70/237), а именно: «Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности публичного ядра интернета и, следовательно, стабильности киберпространства»*.

Общество интернета: *«Публичное ядро интернета включает в себя системы маршрутизации, именования и нумерации интернета (систему доменных имен), криптографические механизмы безопасности и идентификации, а также кабели связи. Это основные функциональные элементы, которые делают интернет работоспособным, и их необходимо защищать, чтобы интернет оставался технологией, обеспечивающей глобальный охват и целостность. Мы призываем РГОС должным образом учесть ценности нормы GCSC для защиты публичного ядра, в которой подчеркивается необходимость того, чтобы как государственные, так и негосударственные субъекты воздерживались от выдачи разрешений на ведение какой-либо деятельности, способной нанести преднамеренный или существенный ущерб общей доступности или целостности публичного ядра интернета, а значит и стабильности киберпространства».*

Microsoft: в своем первом комментарии заявляет следующее: *«решительно поддерживает несколько норм, предложенных государствами-членами, которые мы считаем крайне важными дополнениями существующих основополагающих норм деятельности в киберпространстве, ранее согласованных в контексте*

ГПЭ: Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности публичного ядра интернета и, следовательно, стабильности киберпространства». Государственные и негосударственные субъекты не должны ни вести, ни сознательно разрешать деятельность, которая преднамеренно наносит существенный ущерб общедоступности или целостности публичного ядра интернета и, следовательно, стабильности киберпространства».

Во втором комментарии Microsoft сказано следующее: *«Предыдущие обязательства ГПЭ отражают эту важность, и различные последующие заявления, в том числе на конференции Paris Call и в GCSC, отражают растущую приверженность защите технологии, которая лежит в основе самого интернета, от кибератак. В рамках некоторых усилий это упоминается как защита общедоступности или целостности «публичного ядра» интернета, а некоторые предпочитают обращаться к техническим компонентам интернета. Важно отметить, что государства должны согласовать новую норму для защиты тех центральных компонентов, без которых глобальный интернет перестал бы работать. GCSC определяет эти компоненты как: маршрутизацию и пересылку пакетов; системы именования и нумерации; криптографические механизмы безопасности и идентификации; среду передачи, программное обеспечение и дата-центры».*

Двенадцать НПО[12] опубликовали совместное заявление: *«Атаки на критически важную инфраструктуру, а в данном случае и на «наднациональную критически важную информационную инфраструктуру» (под которой следует понимать систему доменных имен и другие элементы публичного ядра интернета), представляют собой «угрозу не только безопасности, но также экономическому развитию и жизнедеятельности людей» (пункт 19). Мы предлагаем прямо и четко упомянуть в отчете эти гуманитарные последствия атак на критически важную инфраструктуру и их влияние на права человека».*
и «Мы поддерживаем рекомендацию, изложенную в пункте 38, о необходимости защитить общедоступность и целостность публичного ядра интернета, которую следует понимать как дальнейшую подготовку спецификации или уточнение уже согласованных ГПЭ в 2015 году норм защиты критически важной инфраструктуры.Публичное ядро — это критически важные элементы инфраструктуры интернета, а именно: маршрутизация и пересылка пакетов; системы именования и нумерации; криптографические механизмы безопасности и идентификации; среда передачи, программное обеспечение и дата-центры».

***

[12]Это следующие 12 НПО:Access Now, Ассоциация прогрессивных коммуникационных технологий, Центр управления средствами связи в Национальном юридическом университете Дели, Derechos Digitales, Fundación Karisma, Global Partners Digital, Кенийская сеть действий в области ИКТ (KICTANet), Международный центр некоммерческого права, R3D: Red en Defensa de los Derechos Digitales, Африканский центр исследований в области ИКТ, Фонд СМИ Западной Африки, Компьютерный учебный центр и цифровая студия YMCA, Гамбия.

27 мая 2020 года председатель РГОС опубликовал[13] пересмотренный предварительный проект отчета и обновленный неофициальный документ,[14] в которых отражены, согласно письму председателя, «новые предложения, полученные по пункту повестки дня "Правила, нормы и принципы"».[15] Этот обновленный предварительный проект отчета и неофициальный документ обсуждались на виртуальном совещании, которое состоялось 15, 17, 19 июня и 2 июля 2020 года. Согласно письму, которое 16 июля 2020 года опубликовал председатель РГОС и постоянный представитель Швейцарии при ООН, посол Юрг Лаубер (Jürg Lauber), график дальнейших неофициальных заседаний для обсуждения предварительного проекта следующий: второй раунд 29 сентября – 1 октября 2020 года; третий раунд 17–19 ноября 2020 года; и четвертый раунд 1–3 декабря 2020 года.[16]

Во втором раунде продолжится обсуждение вопросов международного права, третий будет посвящен мерам укрепления доверия и наращивания потенциала, а четвертый будет сочетанием обычного институционального диалога и общих комментариев. После этого председатель, как ожидается, опубликует нулевой проект отчета (в начале 2021 года), который будет обсуждаться на третьем основном совещании 8–12 марта 2021 года. На момент опубликования письма председателя планом предусмотрено проведение виртуальных или гибридных неофициальных заседаний и очной основной встречи.

Группа правительственных экспертов (ГПЭ)

Не поступило новой информации о работе ГПЭ с момента опубликования нашего документа от 28 февраля 2020 года.[17]

Участие ICANN и дальнейшие действия

Отдел корпорации ICANN по взаимодействию с правительствами организовал и совместно провел 22 апреля 2020 года виртуальный брифинг для дипломатов из постоянных представительств при ООН. Брифинг был проведен постоянными представительствами Болгарии и Эстонии при ООН в Нью-Йорке и Отделением ООН в Женеве. Дэвид Конрад (David Conrad), технический директор ICANN, и Наэла Саррас (Naela Sarras), старший менеджер по службам IANA, выступили с докладами и пообщались со 116 дипломатами, принявшими участие. Они разъяснили роль ICANN в экосистеме интернета и ответили на вопросы дипломатов.

Отдел ICANN по взаимодействию с правительствами по-прежнему будет следить за ходом обсуждений в ООН и должным образом публиковать необходимые отчеты.

[13] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-revised-pre-draft.pdf
[14] https://front.un-arm.org/wp-content/uploads/2020/05/200527-oewg-ict-non-paper.pdf
[15] Письмо опубликовано здесь.
[16] Загрузить письмо (PDF-файл) можно здесь.
[17] https://www.un.org/disarmament/group-of-governmental-experts/

ПРИЛОЖЕНИЕ 1

Справочная информация о комитетах ООН и ГА ООН

Учрежденная 24 октября 1945 года ООН в последнее время все активнее участвует в дискуссиях, которые затрагивают различные вопросы, связанные с интернетом. Генеральная Ассамблея Организации Объединенных Наций в течение многих лет в рамках Первого и Второго комитетов обсуждает резолюции, направленные на кибербезопасность и управление интернетом (IG).[18]

Первый комитет ГА ООН[19] — это комитет, где исторически началось обсуждение первой резолюции, относящейся к киберпространству.[20] В 2018 году были созданы две рабочие группы по кибербезопасности — РГОС[21] и ГПЭ, о которых рассказывалось в документе, опубликованном в феврале 2020 года.[22]

Второй комитет ГА ООН[23] рассматривает вопросы, связанные с интернетом, в рамках резолюции об использовании информационно-коммуникационных технологий (ИКТ) в целях развития.[24] Обсуждение вопросов управления интернетом началось[25] с принятия Генеральной Ассамблеей Организации Объединенных Наций резолюции A/RES/56/183[26] в 2002 году в рамках Всемирной встречи на высшем уровне по вопросам информационного сообщества (ВВУИО). Эта резолюция неоднократно обновлялась в 2003 и 2005 годах при подготовке к ВВУИО в Женеве (2003 год) и Тунисе (2005 год). В период между этапами ВВУИО в Женеве и Тунисе была создана Рабочая группа по управлению интернетом (WGIG), которая опубликовала свой собственный отчет.[27]

На ВВУИО был принят документ «Тунисская программа ВВУИО», который с 2005 года служит одним из ключевых документов, объясняющих (помимо множества других вопросов) модель управления интернетом с участием многих заинтересованных сторон.[28]

Второй комитет ГА ООН ежегодно пересматривает резолюцию по использованию ИКТ в целях обеспечения развития. В 2015 году он также потратил много времени на

---

[18] Как указано выше, ООН не использует термин «кибербезопасность», однако мы используем его в настоящем документе для информационных целей.
[19] http://www.un.org/en/ga/first/index.shtml
[20] Резолюция A/RES/53/70, озаглавленная «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», была предложена в 1998 году.
[21] РГОС занимается вопросами «достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности».
[22] https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en
[23] https://www.un.org/en/ga/second/index.shtml
[24] Начиная с 2018 года, ИКТ в целях обеспечения устойчивого развития, как указано на сайте ЮНКТАД.
[25] ВВУИО впервые обсуждалась МСЭ на его Полномочной конференции 1998 года, и соответствующее решение о проведении ВВУИО было одобрено ГА ООН в 2001 году.
[26] https://unctad.org/en/PublicationsLibrary/ares56d183_en.pdf
[27] См. материалы Государственного департамента США или загрузите PDF-файл с сайта самой группы WGIG.
[28] https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

обсуждение в рамках *ВВУИО+10,* которое привело к опубликованию итогового документа ВВУИО+10[29] и завершилось заседанием ГА ООН высокого уровня 15–16 декабря 2015 года.[30] Итоговый документ, среди прочего, подтвердил модель управления интернетом с участием многих заинтересованных сторон и продлил мандат Форума по управлению интернетом (IGF) еще на десять лет.[31]

Третий комитет ГА ООН[32] начал изучать киберпреступность с принятия в 2019 году резолюции[33] о создании Специального межправительственного комитета экспертов открытого состава (OECE) для начала разработки новой конвенции ООН о борьбе с киберпреступностью.[34]

[29] Сайт ООН не работает, но документ можно найти по его названию: UNPAN95735.pdf
[30] Официальный сайт: https://publicadministration.un.org/wsis10/GA-High-Level-Meeting
[31] https://www.intgovforum.org/multilingual/
[32] https://www.un.org/en/ga/third/index.shtml
[33] Документ доступен для загрузки на одном из языков ООН здесь.
[34] Полное название этой группы: «Специальный межправительственный комитет экспертов открытого состава, представляющий все регионы, для разработки всеобщей международной конвенции о противодействии использованию информационных и коммуникационных технологий в преступных целях».