О деятельности ООН в сфере кибербезопасности

Отчет о дискуссиях в ООН, связанных с вопросами в сфере кибербезопасности

Вени Марковски (Veni Markovski)
Алексей Трепыхалин (Alexey Trepykhalin)
3 июня 2021
GE-009

ICANN

СОДЕРЖАНИЕ

Введение

В этом документе представлен отчет о работе различных групп Генеральной Ассамблеи Организации Объединенных Наций (ГА ООН), где обсуждаются вопросы, связанные с кибербезопасностью. Он содержит свежую информацию о ходе обсуждений в первой Рабочей группе открытого состава (РГОС), Группе правительственных экспертов (ГПЭ) и Специальном комитете экспертов открытого состава (АНС[1]) в период с 1 июля 2020 года по 3 июня 2021 года.

Этот документ входит в состав серии регулярных отчетов, содержащих обзор деятельности в ООН, которая имеет отношение к экосистеме интернета и миссии ICANN.[2] Мониторинг такой деятельности демонстрирует готовность и обязанность отдела по взаимодействию с правительствами и межправительственными организациями (GE) корпорации ICANN информировать все сообщество ICANN о вопросах, представляющих важность для глобального единого функционально совместимого интернета и его системы уникальных идентификаторов.[3]

Отчет о деятельности Рабочей группы открытого состава (РГОС)

За период, прошедший после публикации корпорацией ICANN в июле 2020 года отчета об имеющих отношение к кибербезопасности дискуссиях в ООН, РГОС провела в том году еще три раунда неофициальных консультаций (29 сентября – 1 октября, 17–19 ноября и 1–3 декабря). В ходе этих консультаций секретариат РГОС получил ряд комментариев и предложений от государств-членов в рамках официального процесса, а также от неправительственных организаций в рамках инициированных председателем РГОС неофициальных консультаций.

Ниже представителями отдела GE корпорации ICANN представлена сводная информация только о тех поступивших в РГОС предложениях, которые касаются миссии ICANN. Список этих предложений отсортирован по дате.

2 июля 2020 года, Финляндская Республика: «Мы также хотим решительно поддержать предложение Нидерландов о защите целостности и доступности публичного ядра интернета, в том числе конкретные предложения относительно сферы применения норм для критической инфраструктуры (13f и 13g)».[4]

---

[1] В двух предыдущих отчетах мы использовали аббревиатуру OECE, но на первом заседании комитета заметили, что государства-члены ООН используют для обозначения Специального комитета другую аббревиатуру — АНС. Поэтому корпорация ICANN соответствующим образом скорректировала терминологию в интересах единообразия. Полное название этого комитета «Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях».

[2] Предыдущие отчеты GE см. здесь: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en Этот и все остальные URL в сносках и приложениях были загружены 3 июня 2021 года.

[3] «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

[4] «Заявления Финляндской Республики», Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности,

19 ноября 2020 года, Исламская Республика Иран: «Эти [односторонние] цифровые санкции повлияли на инвестиции в объекты инфраструктуры ИКТ, а также на доступ к цифровым технологиям и ресурсам, таким как IP-адреса, система и сети DNS, что не только препятствует достижению национальных целей развития в области ИКТ, но и нарушает права человека».[5]

19 января 2021 года, Королевство Нидерландов: «Положение о том, что "государственные и негосударственные субъекты не должны вести или сознательно допускать деятельность, которая намеренно и существенно нарушает общедоступность или целостность публичного ядра интернета и, следовательно, стабильность киберпространства" [будет] практическим принципом реализации рекомендации ГПЭ ООН № 13(f) от 2015 года и вследствие этого также относится к сфере, охватываемой рекомендацией ГПЭ ООН № 13(g) от 2015 года».[6]

19 февраля 2021 года, Республика Словения: «Мы также хотели бы поддержать призывы Нидерландов уделять больше внимания защите публичного ядра интернета».[7]

19 февраля 2021 года, Федеративная Республика Германия: «Предлагается включить в раздел о существующих и потенциальных угрозах ссылку на угрозы публичному ядру интернета, которые также упоминаются в параграфе 50 Проекта 0».[8]

19–22 февраля 2021 года, Королевство Нидерландов: «С течением лет деятельность в киберпространстве, направленная на нарушение целостности, функционирования и доступности интернета, стала реальной и значимой угрозой. В данном контексте в предварительном проекте доклада РГОС используется термин "публичное ядро". Стремясь к консенсусу, мы связались со странами, выразившими озабоченность во время предыдущих дискуссий, и пришли к новой формулировке, которая, по-видимому, снимает эту озабоченность. Это следующая формулировка: «техническая инфраструктура, необходимая для обеспечения общедоступности или целостности интернета"».[9]

виртуальные неофициальные консультации, 19 июня и 2 июля 2020 года, https://front.un-arm.org/wp-content/uploads/2020/09/oewg-informal-virtual-meetings-statement-by-finland-19-june-and-2-july-2020.pdf

[5] «Пересмотренный предварительный проект доклада РГОС», третье неофициальное виртуальное совещание РГОС, выступление делегации Исламской Республики Иран «Наращивание потенциала», 19 ноября 2020 года, https://front.un-arm.org/wp-content/uploads/2020/11/iran-intervention-on-capacity-building-19-nov-2020.pdf

[6] «Неофициальный документ с перечнем конкретных предложений по пункту повестки дня "Правила, нормы и принципы", составленный на основе письменных заявлений делегаций», в редакции от 18 января 2021 года, https://front.un-arm.org/wp-content/uploads/2021/01/OEWG-Non-paper-rules-norms-and-principles-19-01-2021.pdf

[7] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, неофициальное виртуальное совещание (18, 19 и 22 февраля 2021 года), заявление Словении, 19 февраля 2021 года, https://front.un-arm.org/wp-content/uploads/2021/02/Slovenia-19-February-2021-FINAL.pdf

[8] Комментарии Германии к Проекту 0 доклада РГОС, 19 февраля 2021 года, https://front.un-arm.org/wp-content/uploads/2021/02/Germany-Written-Contribution-OEWG-Zero-Draft-Report_clean.pdf

[9] Адресованное ООН заявление Её Превосходительства Натали Яарсма (Nathalie Jaarsma), Королевство Нидерландов, (18,19 и 22 февраля 2021 года), https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-informals-intervention-Feb-2021.pdf

23 февраля 2021 года, Великобритания: «Мы выражаем благодарность Нидерландам за работу вместе с нами и другими лицами над уточнением их предложения по "публичному ядру" и приветствуем включение компромиссного текста».[10]

25 февраля 2021 года, Королевство Нидерландов: «В соответствии с текстом о защите публичного ядра, который был включен в предварительный проект, учитывая сближение позиций относительно точной формулировки, мы предлагаем следующее. Мы хотели бы предложить изменить формулировку в последнем предложении параграфа 21 "целостность, функционирование и доступность" на [настоятельную потребность защиты] "технической инфраструктуры, необходимой для обеспечения общедоступности или целостности интернета"».

«Кроме того, мы хотели бы упомянуть о важности "защиты технической инфраструктуры, необходимой для обеспечения общедоступности или целостности интернета" в разделе "Вывод и рекомендация" правил, норм и принципов».[11]

3 марта 2021 года, Глобальная комиссия по стабильности в киберпространстве (GCSC): «Хотя Комиссия с большим удовлетворением отметила, что в предыдущем предварительном проекте доклада был учтен ряд рекомендаций GCSC, мы сожалеем, что многие из этих рекомендаций не включены в Проект 0 или текущий первый проект. В частности, это относится к норме для защиты публичного ядра интернета, получившей, по нашему мнению, положительную оценку со стороны многих государств, а также наблюдателей из гражданского общества и частного сектора».[12]

8 марта 2021 года, Исламская Республика Иран: «Необходимо обеспечить подотчетность платформ и транснациональных корпораций, таких как ICANN».[13]

8 марта 2021 года, Cybersecurity Tech Accord (Технологическое соглашение по кибербезопасности): «Недавний взлом SolarWinds показал, что ни одна организация не должна считать себя защищенной от достаточно обеспеченного ресурсами и решительного противника. Это также продемонстрировало беззастенчивую готовность продвинутых злоумышленников подрывать доверие к важнейшим процессам и публичному ядру интернета посредством осуществления атаки».[14]

---

[10] Комментарии Великобритании к Проекту 0 доклада РГОС по достижениям в сфере ИКТ в контексте международной безопасности, 23 февраля 2020 года, https://front.un-arm.org/wp-content/uploads/2021/02/UK-submission-to-OEWG-ICTs-zero-draft-002.pdf

[11] Нидерланды — письменные предложения по Проекту 0 доклада РГОС, февраль 2021 года, https://front.un-arm.org/wp-content/uploads/2021/02/Netherlands-OEWG-written-comments-to-zero-draft.pdf

[12] Комментарии GCSC к первому проекту основного доклада Рабочей группы открытого состава, 3 марта 2021 года, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Submission-to-OEWG-First-Draft-Report-March-2021.pdf

[13] Первое заседание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия (8–12 марта 2021 года), веб-телевидение ООН, 8 марта 2021 года, (начинается с 1:29:40) https://media.un.org/en/asset/k1o/k1obxycc3u

[14] Ответ Cybersecurity Tech Accord на основной доклад РГОС ООН [ПЕРВЫЙ ПРОЕКТ], https://front.un-arm.org/wp-content/uploads/2021/03/Tech-Accord-OEWG-response-March-2021-FINAL.pdf

9 марта 2021 года Федеративная Республика Германия поддержала новую компромиссную формулировку «... в частности, что касается публичного ядра интернета».[15]

9 марта 2021 года коалиция из девяти организаций гражданского общества рекомендовала включить в доклад РГОС: «...упоминание о необходимости того, чтобы все участники защищали базовую доступность и целостность глобального интернета, что включает невмешательство в публичное ядро интернета».[16]

10 марта 2021 года, Китайская Народная Республика: «Государства должны участвовать в управлении и распределении международных интернет-ресурсов на равной основе».[17]

12 марта 2021 года GCSC выразила «сожаление по поводу отсутствия термина "публичное ядро" в окончательном проекте доклада РГОС».[18]

В дополнение к итоговому докладу РГОС председатель РГОС опубликовал резюме, содержавшее предыдущую формулировку о публичном ядре, предложенную Нидерландами 19 января.[19]

Компромиссный текст итогового доклада РГОС 2021 года с новой формулировкой пунктов 18 и 26, согласованной государствами-членами, гласит следующее:

«18. Государства пришли к выводу, что злонамеренная деятельность с использованием ИКТ против объектов критической инфраструктуры (CI) и критической информационной инфраструктуры (CII), обеспечивающих оказание населению социально значимых услуг, может привести к разрушительным последствиям в области безопасности, а также в экономической, социальной и гуманитарной областях. Хотя определение того, какие виды инфраструктуры считаются критически важными, является прерогативой каждого государства, такая инфраструктура может включать медицинские учреждения, финансовые службы, энергетику, водоснабжение, транспорт и санитарию. Направленная против CI и CII злонамеренная деятельность с использованием ИКТ, которая подрывает доверие к политическим и избирательным

[15] Третье заседание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия (8–12 марта 2021 года), веб-телевидение ООН, 8 марта 2021 года, (начинается с 38:20), https://media.un.org/en/asset/k13/k13uzdidth

[16] «Совместный отзыв гражданского общества о первом проекте доклада РГОС по ИКТ», архив документов РГОС, 9 марта 2021 года, https://front.un-arm.org/wp-content/uploads/2021/03/Joint-CS-feedback-on-first-draft-1.pdf

[17] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия, 8–12 марта 2021 года, Резюме председателя РГОС, рабочий документ заседания, 10 марта 2021 года, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

[18] Заявление GSCS относительно окончательного проекта основного доклада Рабочей группы открытого состава ООН, 12 марта 2021 года, https://front.un-arm.org/wp-content/uploads/2021/03/GCSC-Statement-OEWG-Multistakeholder-Consultation-Final-Draft-Report-March-2021.pdf

[19] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия, 8–12 марта 2021 года, Резюме председателя, рабочий документ заседания, 10 марта 2021 года, A/AC.290/2021/CRP.3*, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

процессам, государственным учреждениям или оказывает негативное воздействие на общедоступность или целостность интернета, также является реальной и все более серьезной проблемой. Такой инфраструктурой может владеть или управлять частный сектор; она может использоваться совместно с другим государством или эксплуатироваться в разных государствах. Вследствие этого может возникать необходимость межгосударственного или государственно-частного сотрудничества для защиты ее целостности, работоспособности и доступности».[20]

«26. Признавая необходимость защиты всех объектов критической инфраструктуры (CI) и критической информационной инфраструктуры (CII), обеспечивающих оказание населению социально значимых услуг, а также стремясь гарантировать общедоступность и целостность интернета, государства также пришли к выводу, что пандемия COVID-19 подчеркнула важность защиты инфраструктуры здравоохранения, в том числе медицинских служб и учреждений, путем введения норм, касающихся критической инфраструктуры, например тех, которые были утверждены на основе консенсуса в резолюции 70/237 Генеральной Ассамблеи ООН».[21]

Делегация Нидерландов в своих комментариях к одобренному на основе консенсуса докладу РГОС отметила, что «Нидерланды тепло приветствуют включение в документ текста об общедоступности и целостности интернета — того, что мы считаем публичным ядром интернета».[22]

Отчет о деятельности Группы правительственных экспертов (ГПЭ)

28 мая 2021 года на основе консенсуса был принят доклад ГПЭ.[23] Ряд моментов в этом докладе имеет отношение к сообществу ICANN в глобальном контексте дискуссий в ООН, связанных с кибербезопаностью, свидетелями которых мы стали в последние несколько лет. Приведенные ниже цитаты (в некоторых случаях цитирование частичное) взяты из *уведомительной копии доклада Группы правительственных экспертов по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности* и «сопроводительного письма» к этому докладу.[24]

[20] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, итоговый основной доклад, рабочий документ заседания, 10 марта 2021 года, A/AC.290/2021/CRP.2, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

[21] Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, итоговый основной доклад, рабочий документ заседания, 10 марта 2021 года, A/AC.290/2021/CRP.2.

[22] Девятое заседание Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третья основная сессия (8–12 марта 2021 года), веб-телевидение ООН, 12 марта 2021 года, (начинается с 35:23), https://media.un.org/en/asset/k1r/k1rf2exuhz

[23] Сообщение Государственного департамента США в Твиттере, 28 мая 2021 года, https://twitter.com/State_Cyber/status/1398314450743091201?s=20

[24] Доклад Группы правительственных экспертов по продвижению ответственного поведения государств в киберпространстве в контексте международной безопасности, уведомительная копия и сопроводительное письмо, 28 мая 2021 года, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf

Пункт 10: «Вредоносная деятельность с использованием ИКТ против критической инфраструктуры, которая обеспечивает предоставление услуг внутри страны, на региональном или глобальном уровне, все больше внушает опасения, о чем говорилось в предыдущих докладах ГПЭ. Особую озабоченность вызывает злонамеренная деятельность с использованием ИКТ, затрагивающая критическую информационную инфраструктуру, инфраструктуру предоставления социально значимых услуг населению, техническую инфраструктуру, необходимую для обеспечения общедоступности или целостности интернета, а также для работы организаций из сектора здравоохранения».

Пункт 17: «Группа также приняла к сведению предложение Китая, Казахстана, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана о международном кодексе поведения в области обеспечения информационной безопасности (см. A / 69/723)».[25]

Пункт 44: «Как отмечается в норме 13 (g), государства должны принимать надлежащие меры для защиты своей критической инфраструктуры. В этой связи каждое государство определяет, какие виды инфраструктуры или сектора оно считает критически важными в пределах своей юрисдикции, в соответствии с национальными приоритетами и методами классификации критической инфраструктуры».

Пункт 45: «Критическая инфраструктура может также относиться к тем видам инфраструктуры, которые обеспечивают предоставление услуг в нескольких государствах, таким как техническая инфраструктура, необходимая для общедоступности или целостности интернета».

Пункт 48: «Определение государством критически важных видов инфраструктуры или секторов может быть полезным для защиты указанной инфраструктуры или сектора. В дополнение к определению видов или секторов инфраструктуры, считающихся критически важными, каждое государство определяет структурные, технические, организационные, законодательные и нормативные меры, необходимые для защиты своей критической инфраструктуры и восстановления ее функций при возникновении инцидентов».

Пункт 49: «В некоторых государствах размещена инфраструктура, обеспечивающая предоставление услуг на региональном или международном уровнях. Угрозы ИКТ для такой инфраструктуры могут иметь дестабилизирующие последствия. Государства, участвующие в таких соглашениях, могли бы поощрять трансграничное сотрудничество с соответствующими владельцами и операторами инфраструктуры с целью усиления мер безопасности в области ИКТ, предусмотренных для такой инфраструктуры, и укрепления существующих или разработки дополнительных процессов и процедур выявления и смягчения последствий инцидентов в области ИКТ, затрагивающих такую инфраструктуру».

Пункт 63: «Кроме того, по согласованию с участниками соответствующей отрасли и другими субъектами, занимающимися вопросами безопасности ИКТ, государства могут разработать руководящие указания и стимулы, соответствующие применимым международным техническим стандартам, для ответственного представления

[25]Приложение к письму постоянных представителей Китая, Казахстана, Кыргызстана, Российской Федерации, Таджикистана и Узбекистана при ООН от 9 января 2015 года на имя Генерального секретаря [Оригинал: на китайском и русском языках], Правила поведения в области обеспечения международной информационной безопасности, A/69/723, https://documents-dds-ny.un.org/doc/UNDOC/GEN/N15/014/02/PDF/N1501402.pdf?OpenElement

отчетности и управления уязвимостями, а также определить роли и обязанности различных заинтересованных сторон в процессах подготовки отчетности, виды технической информации, подлежащей раскрытию или опубликованию, включая обмен технической информацией о серьезных инцидентах в сфере ИКТ, и порядок обращения с данными, требующими особенного внимания, и обеспечения безопасности и конфиденциальности информации».

Пункт 79: «Диалог в формате двусторонних, субрегиональных, региональных и многосторонних консультаций и взаимодействия может способствовать взаимопониманию между государствами, укреплению доверия и более тесному сотрудничеству между государствами в области сокращения количества инцидентов в сфере ИКТ при одновременном снижении рисков неправильного восприятия и эскалации. Другие заинтересованные стороны, такие как частный сектор, сектор науки и образования, гражданское общество и техническое сообщество, могут внести значительный вклад, способствующий таким консультациям и взаимодействию».

Пункт 87: «Группа подчеркивает важность сотрудничества, оказания помощи и наращивания потенциала в области безопасности ИКТ в контексте всех пунктов мандата Группы. Расширение сотрудничества наряду с более эффективной помощью и наращиванием потенциала в области безопасности ИКТ с привлечением других заинтересованных сторон, таких как частный сектор, сектор науки и образования, гражданское общество и техническое сообщество, может содействовать применению государствами концепции ответственного поведения при использовании ИКТ. Они имеют решающее значение для преодоления существующих внутригосударственных и межгосударственных разногласий по политическим, правовым и техническим вопросам, имеющим отношение к безопасности ИКТ. Они также могут способствовать достижению других целей международного сообщества, таких как ЦУР».

Пункт 95: «Группа также определила потенциальные направления будущей работы, к которым помимо прочего относится: [...] г) Выявление механизмов, способствующих вовлечению других важных заинтересованных сторон, включая частный сектор, сектор науки и образования, гражданское общество и техническое сообщество, в работу по внедрению концепции ответственного поведения, когда это необходимо».

Отчет о деятельности Специального комитета экспертов открытого состава (АНС)

Планировалось, что АНС приступит к работе в августе 2020 года, но из-за пандемии COVID-19 его первая организационная сессия прошла 10–12 мая 2021 года.[26] За период после подготовки в июле 2020 года документа корпорации ICANN на веб-странице АНС было опубликовано несколько новых материалов.[27] На первом

[26] Видеозапись заседаний организационной сессии АНС доступна для просмотра здесь:
Первое заседание: https://media.un.org/en/asset/k1v/k1vgo4a624 (Второе заседание не проводилось, поскольку все организационные вопросы были решены на первом заседании.)
Третье заседание: https://media.un.org/en/asset/k1z/k1zsp4exqc
Четвертое заседание: https://media.un.org/en/asset/k12/k12bsxlcak
Пятое заседание: https://media.un.org/en/asset/k1m/k1ma80pf1p
Шестое заседание: https://media.un.org/en/asset/k1m/k1m0si6d6n

[27] «Специальный комитет, созданный на основании резолюции 74/247 Генеральной ассамблеи», UNODC, https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

заседании организационной сессии 10 мая 2021 года АНС избрал председателя комитета, докладчика и 13 заместителей председателя, представляющих различные географические регионы.[28] АНС не смог достичь консенсуса в отношении порядка проведения своих будущих заседаний в отведенное время, и председатель объявил, что позже состоятся неофициальные консультации.[29]

26 мая 2021 года на своем 71-м пленарном заседании Генеральная Ассамблея ООН приняла без голосования текст резолюции A/RES/75/282 «Противодействие использованию информационных и коммуникационных технологий в преступных целях».[30] В документах определены два места проведения сессий АНС: Вена и Нью-Йорк. Всего состоится семь сессий с ротацией места проведения между Веной и Нью-Йорком. Первая и последняя сессии состоятся в штаб-квартире ООН в Нью-Йорке. Решения АНС по существенным вопросам без одобрения на основе консенсуса принимаются большинством в две трети присутствующих и участвующих в голосовании представителей.

Также в этой резолюции председателю АНС рекомендовано проводить межсессионные консультации с целью получения материалов для разработки проекта конвенции от широкого круга заинтересованных сторон.

Заключение

Специалисты отдела GE по-прежнему будут следить за ходом обсуждений в АНС и новой РГОС, которая будет выполнять свою работу с 2021 по 2025 год. РГОС провела свое первое организационное заседание 1 июня 2021 года, на котором избрала председателем постоянного представителя Сингапура при ООН.[31]

Отчеты о работе РГОС, ГПЭ, АНС, а также другие опубликованные отделом GE документы доступны на веб-странице GE корпорации ICANN.[32]

---

[28] Организационная сессия Специального комитета была проведена 10–12 мая 2021 года в Нью-Йорке. Результаты избрания должностных лиц Специального комитета: https://www.unodc.org/unodc/en/cybercrime/cybercrime-adhoc-committee.html

[29] Шестое заседание Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, веб-телевидение ООН, 12 мая 2021 года, (начинается с 3:24:34) https://media.un.org/en/asset/k18/k18lkzt0oq

[30] Резолюция, принятая Генеральной Ассамблеей 26 мая 2021 года, «75/282. Противодействие использованию информационных и коммуникационных технологий в преступных целях», дата распространения: 1 июня 2021 года, A/RES/75/282, https://undocs.org/a/res/75/282

[31] 1 июня, 1-е заседание: https://media.un.org/en/asset/k1o/k1oa2ngbsc
1 июня, 2-е заседание: https://media.un.org/en/asset/k14/k1443my9hu

[32] Веб-страница GE, сайт ICANN: https://www.icann.org/resources/pages/government-engagement-publications-2020-03-02-en

Приложение

РГОС. Итоговый основной отчет: https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

РГОС. Резюме председателя: Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, третье основное заседание 8–12 марта 2021 года https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

РГОС. Видеоматериалы третьего основного заседания, 8–12 марта 2021 года

8 марта 2021 года
День 1. 1-е заседание
https://media.un.org/en/asset/k1o/k1obxycc3u

День 1. 2-е заседание
https://media.un.org/en/asset/k18/k1893g1q0h

9 марта 2021 года
День 2. 3-е заседание
https://media.un.org/en/asset/k13/k13uzdidth

День 2. 4-е заседание
https://media.un.org/en/asset/k1h/k1huoxryeo

10 марта 2021 года
День 3. 5-е заседание
https://media.un.org/en/asset/k1d/k1d4e06j0x

День 3. 6-е заседание
https://media.un.org/en/asset/k1m/k1mqlxrfv4

11 марта 2021 года
День 4. 7-е и 8-е заседания не состоялись. Этот день был выделен для двусторонних обсуждений и консультаций со столицами.

12 марта 2021 года
День 5. 9-е заседание
https://media.un.org/en/asset/k1r/k1rf2exuhz

День 5. 10-е заседание (На сайте ООН отсутствует ссылка на видеозапись этого заседания).

День 5. 11-е заседание — заключительное заседание РГОС (принятие основного отчета на основе консенсуса) https://media.un.org/en/asset/k1p/k1prn29un6