



Генеральная Ассамблея

Distr.: General

21 May 2024

Russian

Original: Chinese/English/French/
Russian/Spanish

Семьдесят девятая сессия

Пункт 93 первоначального перечня*

**Достижения в сфере информатизации
и телекоммуникаций в контексте международной
безопасности****Достижения в сфере информатизации
и телекоммуникаций в контексте международной
безопасности****Доклад Генерального секретаря***Резюме*

В настоящем докладе приводится резюме элементов, выделенных при анализе материалов, которые были получены государствами-членами в соответствии с резолюцией 78/237, без ущерба для их индивидуальных позиций. В нем обобщены мнения государств относительно безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, в первую очередь в отношении будущего регулярного институционального диалога по этим вопросам под эгидой Организации Объединенных Наций. Мнения, полученные от государств-членов к установленному сроку, в полном объеме приводятся в приложении к настоящему докладу. В заключительной части доклада приводятся замечания Генерального секретаря.

* A/79/50



Содержание

	<i>Стр.</i>
I. Введение	3
II. Справочная информация	3
III. Мнения о регулярном институциональном диалоге по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий	4
IV. Замечания и выводы Генерального секретаря	11
Приложение	
Ответы, полученные от правительств	14
Австралия	14
Азербайджан	18
Канада	20
Китай	22
Куба	24
Чехия	25
Дания	27
Египет	29
Эстония	33
Франция	36
Грузия	43
Германия	44
Ирландия	48
Япония	50
Латвия	53
Нидерланды (Королевство)	56
Новая Зеландия	59
Российская Федерация	60
Сингапур	63
Турция	64
Соединенные Штаты Америки	89
Венесуэла (Боливарианская Республика)	96
Ответы, полученные от межправительственных организаций	97
Европейский союз	97

I. Введение

1. В пункте 8 резолюции [78/237](#) Генеральная Ассамблея просила все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, в частности в отношении будущего регулярного институционального диалога по данным вопросам под эгидой Организации Объединенных Наций, и просила Генерального секретаря представить доклад на основе этих мнений Генеральной Ассамблее в ходе ее семьдесят восьмой сессии для дальнейшего обсуждения государствами-членами на заседаниях рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 в ходе ее восьмой сессии в 2024 году. Настоящий доклад представляется во исполнение этой просьбы.
2. 5 января 2023 года Управление по вопросам разоружения направило всем государствам-членам вербальную ноту, в которой обратило их внимание на содержание пункта 8 резолюции [78/237](#) и предложило представить мнения по этому вопросу. Ответы, полученные по состоянию на 1 мая 2024 года, воспроизводятся в приложении к настоящему докладу. Ответы, полученные после этой даты, размещены на онлайн-портале заседаний Управления по вопросам разоружения¹.
3. В разделе II настоящего доклада приводится справочная информация, касающаяся обсуждения государствами вопроса о регулярном институциональном диалоге по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. В разделе III приводится резюме элементов, выделенных при анализе материалов, которые были получены от государств-членов, без ущерба для их индивидуальных позиций. В разделе IV изложены замечания и выводы Генерального секретаря.

II. Справочная информация

4. Под эгидой рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 государства продолжают обсуждать, в соответствии с согласованной повесткой дня рабочей группы, содержащейся в документе [A/AC.292/2021/1](#), вопрос о налаживании под эгидой Организации Объединенных Наций регулярного институционального диалога по соответствующим вопросам с широким кругом государств-участников. В ходе семи основных сессий рабочей группы с декабря 2021 года по март 2024 года государства провели предметные обсуждения в целях дальнейшего рассмотрения предложений, касающихся регулярного институционального диалога, включая предложение относительно программы действий.
5. В своем втором ежегодном докладе о работе, проделанной рабочей группой, который был принят консенсусом в июле 2023 года ([A/78/265](#)), государства, договорившись продолжить обсуждение дополнительных элементов, в принципе согласились с тем, что будущий механизм регулярного институционального диалога будет основываться на следующих общих элементах:
 - а) это будет одновекторный, возглавляемый государствами постоянный механизм под эгидой Организации Объединенных Наций, подотчетный Первому комитету Генеральной Ассамблеи;

¹ <https://meetings.unoda.org/ga-c1/general-assembly-first-committee-seventy-ninth-session-2024>.

b) целью будущего механизма будет дальнейшее содействие созданию открытой, безопасной, стабильной, доступной, мирной и функционально совместимой информационно-коммуникационной среды;

c) в основу работы будущего механизма будут положены консенсусные договоренности о рамках ответственного поведения государств при использовании информационно-коммуникационных технологий, содержащиеся в предыдущих докладах рабочей группы открытого состава и Группы правительственных экспертов;

d) это будет открытый, инклюзивный, транспарентный, устойчивый и гибкий процесс, способный развиваться в соответствии с потребностями государств, а также с учетом изменений в среде информационно-коммуникационных технологий.

6. Государства далее особо отметили важность принципа консенсуса как в отношении учреждения самого будущего механизма, так и в отношении процессов принятия решений в рамках этого механизма. Кроме того, государствам, которые имеют такую возможность, было рекомендовано рассмотреть вопрос о создании или поддержке спонсорских программ и других механизмов для обеспечения широкого участия в соответствующих процессах в рамках Организации Объединенных Наций.

7. В ходе проводившихся рабочей группой открытого состава обсуждений, посвященных будущему регулярному институциональному диалогу по вопросам, касающимся безопасности информационно-коммуникационных технологий, государства анализировали его предполагаемые сферу охвата и цели, структуру, формат, в том числе с точки зрения принятия решений, и последующие меры по осуществлению. В целях содействия проведению обсуждений Председатель рабочей группы открытого состава представил в феврале 2024 года дискуссионный документ по проекту элементов постоянного механизма по безопасности информационно-коммуникационных технологий, а затем, в мае 2024 года, — его пересмотренный вариант. Во втором ежегодном докладе о проделанной работе было также предложено провести два специальных межсессионных совещания по теме регулярного институционального диалога. На этих совещаниях государства должны также в целевом порядке провести обсуждения по вопросу о взаимосвязи между программой действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности и деятельностью рабочей группы открытого состава².

III. Мнения о регулярном институциональном диалоге по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий

Общие представления и принципы

8. В представленных ими сообщениях несколько государств особо отметили угрозу, создаваемую злонамеренными действиями при использовании информационно-коммуникационных технологий, и констатировали растущую озабоченность международного сообщества в связи с потенциальными угрозами между-

² См. A/78/76.

народной безопасности и стабильности. Была выражена обеспокоенность по поводу чрезмерного развития рядом государств потенциала информационно-коммуникационных технологий в целях, несовместимых с международным правом и задачами поддержания международной стабильности и безопасности. Было отмечено, что действия отдельных субъектов с использованием информационно-коммуникационных технологий нарушали принципы международного права. Наряду с этим была выражена озабоченность по поводу последствий злонамеренной деятельности для безопасности и благополучия людей.

9. Ряд государств отметили, что информационно-коммуникационные технологии могут стать катализатором прогресса и развития человечества, но одновременно было отмечено, что такие технологии могут использоваться в целях, несовместимых с задачами поддержания международной безопасности, и негативно влиять на экономическое и социальное развитие.

10. Многие государства особо отметили, что в свете нынешней обстановки в плане безопасности необходимо, чтобы будущий регулярный институциональный диалог по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий был направлен на дальнейшее содействие созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Некоторые государства также обратили особое внимание на важность международного сотрудничества между государствами в целях поддержания международной стабильности в этой области.

11. Многие государства отметили, что потребность в создании постоянного механизма принятия решений по соответствующим вопросам под эгидой Организации Объединенных Наций растет. Помимо этого, многие государства также обратили особое внимание на важность развития договоренностей, достигнутых в рамках предыдущих процессов под эгидой Организации Объединенных Наций, в том числе в рамках деятельности группы правительственных экспертов и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности³. Некоторые государства подчеркнули необходимость развивать эту «коллективную нормативную базу», отметив, что ее составляющими элементами являются существующие нормы ответственного использования государством информационно-коммуникационных технологий, применимость международного права к использованию государством этих технологий, меры по укреплению доверия и наращивание потенциала. Было также озвучено мнение о том, что будущий механизм должен создать пространство для более углубленного обсуждения вопроса о практической реализации ранее достигнутых договоренностей. В этой связи было также высказано мнение о том, что неотъемлемым компонентом будущего механизма должен стать межправительственный реестр контактных пунктов.

12. Несколько государств особо отметили важность обеспечения преемственности с точки зрения консенсуса, достигнутого в ходе предыдущих процессов. Высказавшись в том же ключе, несколько государств отметили, что новый институциональный механизм или платформа должны быть созданы по истечении срока действия мандата нынешней рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Некоторые государства акцентировали внимание на том, что в целях обеспечения преемственности это должно быть сделано не позднее 2026 года.

13. Несколько государств особо отметили, что важно избегать дублирования международных усилий в этой области, и предостерегли от работы параллельно

³ См. A/65/201, A/68/98, A/70/174, A/75/816 и A/76/135.

по нескольким направлениям, указав на то, что это ограничивает возможности делегаций. Многие государства подчеркнули важную роль одновекторного, постоянного и инклюзивного регулярного институционального диалога под эгидой Организации Объединенных Наций. Некоторые государства отметили, что создание единого, инклюзивного, постоянно действующего механизма будет также способствовать предсказуемости и институциональной стабильности, избавляя от необходимости регулярно согласовывать новые мандаты. Было также отмечено, что малые и развивающиеся государства, имеющие ограниченные ресурсы, не смогут на устойчивой основе участвовать в двухвекторных параллельных процессах. Кроме того, было высказано мнение, что будущий механизм должен служить комплексным универсальным средством решения проблем в плане безопасности информационно-коммуникационных технологий.

14. Некоторые государства подтвердили, что нормы международного права, в частности Устав Организации Объединенных Наций, применимы и необходимы для поддержания мира, безопасности и стабильности в информационно-коммуникационной среде. В этой связи прозвучало мнение о том, что в рамках будущего механизма можно было бы провести более углубленное обсуждение вопроса о порядке применения международного права. Было предложено изучить в рамках будущего механизма возможность создания специального направления работы по этой теме. Было высказано мнение, что будущий механизм мог бы служить инклюзивной основой для обсуждения вопросов международного права, в том числе для обмена мнениями между странами, проведения брифингов экспертов и анализа деятельности в целях наращивания потенциала в этой области.

15. Государства обсудили различные основополагающие принципы, которые должны составлять основу будущего механизма регулярного институционального диалога по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, включая принципы открытости, инклюзивности и прозрачности, а также тот аспект, что такой механизм должен быть ориентирован на действия и быть одновекторным и демократичным по своей природе. Было высказано мнение, что будущий механизм должен действовать под руководством государств и на основе соблюдения таких принципов Устава, как суверенное равенство государств, неприменение силы или угрозы силой и мирное урегулирование споров. Наряду с этим поступило предложение о том, чтобы предусмотреть в рамках механизма надлежащую гибкость и возможность эволюционного развития по мере изменения потребностей государств и появления новых задач в сфере обеспечения безопасности при использовании информационно-коммуникационных технологий.

16. Несколько государств напомнили о предложении относительно учреждения программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Было отмечено, что это предложение нашло отражение в предыдущих докладах соответствующих органов Организации Объединенных Наций, в том числе в консенсусных ежегодных докладах рабочей группы открытого состава. Кроме того, отмечалось, что предложение было поддержано одной из межрегиональных групп государств и эта программа действий может выступить в роли постоянной структуры для обсуждения вопросов информационно-коммуникационных технологий в контексте международной безопасности, которая будет создана по истечении срока действия мандата нынешней рабочей группы открытого состава.

17. Несколько государств отметили, что сразу же по завершении деятельности нынешней рабочей группы, мандат которой действует до конца 2025 года, следует учредить постоянную рабочую группу открытого состава. Как отметили эти государства, нынешняя рабочая группа открытого состава доказала свою эффективность и актуальность в качестве наиболее подходящего формата для такого механизма и для постоянной рабочей группы открытого состава, которая будет принимать решения и будет уполномочена сосредоточить свои усилия на том, чтобы и далее содействовать созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды посредством, в частности, разработки юридически обязательных правил, норм и принципов ответственного поведения государств, а также создания эффективного механизма для их осуществления в качестве элементов будущего универсального договора об обеспечении международной информационной безопасности.

Сфера охвата и цели

18. Многие государства подчеркнули, что главная цель будущего регулярного институционального диалога по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий заключается в том, чтобы содействовать международному миру и безопасности в этой области. Несколько государств отметили, что будущему механизму надлежит содействовать созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Некоторые государства также отметили, что будущий механизм должен способствовать диалогу и сотрудничеству между государствами и содействовать предотвращению конфликтов и недопонимания.

19. Несколько государств сделали особый акцент на том, что в центре внимания будущего институционального механизма должны оставаться принятые консенсусом рекомендации по итогам предыдущих процессов Организации Объединенных Наций, на базе которых был сформирован свод основополагающих принципов ответственного поведения государств в сфере использования информационно-коммуникационных технологий. Несколько государств подчеркнули, что важно содействовать достижению ранее согласованных результатов, тогда как другие отметили, что в рамках будущего механизма следует рассматривать практическое выполнение соглашений, достигнутых рабочей группой открытого состава. Было высказано предложение относительно того, что в рамках будущего механизма можно было бы выработать конкретные рекомендации в целях оказания государствам поддержки в практическом осуществлении согласованной нормативной базы, а также в целях улучшения ее понимания.

20. В своих материалах государства указали на необходимость дальнейшего развития существующей нормативно-правовой базы. Некоторые государства отметили возможные варианты выявления любых недостатков, разработки дополнительных норм или выработки новых правил и юридически обязывающих договоренностей. Несколько государств поддержали идею разработки юридически обязывающего документа, в то время как другие обратили внимание на то, что при необходимости можно будет продолжить разработку и обновление правовой базы в ответ на новые угрозы по мере их эволюции с течением времени. Несколько государств отметили, что этот механизм должен обеспечивать баланс между двумя в равной мере важными аспектами работы: практическим осуществлением существующей правовой базы и ее дальнейшим развитием.

21. Прозвучало мнение о том, что будущий механизм должен действовать, ориентируясь на будущее и с опорой на прошлое, чтобы сосредоточить внимание как на соблюдении, так и на реализации существующих согласованных рамок

ответственного поведения государств при использовании информационно-коммуникационных технологий, в первую очередь на совершенствовании деятельности по наращиванию потенциала и разработке новых норм с учетом последних событий, в том числе на безопасности данных, а также на разработке новых планов действий по наращиванию потенциала и юридически обязывающего документа.

22. Многие государства особо отметили, что центральное место в деятельности будущего механизма должна занимать тема наращивания потенциала. Некоторые государства подчеркнули важность объединения уже осуществляемых усилий, в частности в контексте соответствующих инициатив Международного союза электросвязи и Всемирного банка. Были упомянуты согласованные принципы наращивания потенциала, содержащиеся в приложении ко второму ежегодному докладу о проделанной работе, который был представлен рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025⁴. Несколько государств отметили, что будущий механизм должен способствовать реализации усилий по наращиванию потенциала, в том числе путем обмена информацией о передовой практике. Несколько государств подчеркнули важность целенаправленных усилий с учетом имеющихся потребностей. Было высказано мнение, что функция механизма, связанная с наращиванием потенциала, должна быть непосредственно увязана с теми усилиями, которые государства прилагают на национальном уровне в целях практического осуществления нормативной базы ответственного поведения государств.

23. Наряду с этим поднимался вопрос о возможности создания, с учетом опыта действующих механизмов в рамках других форумов Организации Объединенных Наций, специального механизма финансирования в поддержку соответствующих усилий в области наращивания потенциала. Было предложено создать добровольную межрегиональную «систему партнерства», в рамках которой государства, обладающие разным потенциалом, могли бы совместно работать, объединив свои усилия в целях укрепления сотрудничества и обмена передовым опытом. Прозвучало предложение создать многокомпонентный механизм наращивания потенциала, который включал бы обмен информацией об угрозах, самостоятельное определение потребностей в плане потенциала и сопоставление потребностей с ресурсами, а также механизм обратной связи для обмена соответствующим опытом.

24. Несколько государств отметили, что будущий механизм мог бы служить всеобъемлющей организационной структурой для реализации соответствующих инициатив и усилий в области безопасности информационно-коммуникационных технологий, в том числе в отношении создания межправительственного реестра контактных пунктов.

25. Государства предложили и другие потенциальные направления деятельности, включая выработку общего понимания того, как международное право применяется к использованию информационно-коммуникационных технологий и каким образом существующие нормы могут быть адаптированы с учетом конкретных особенностей, характерных для этой области. Было высказано мнение, что будущий механизм мог бы способствовать обсуждению существующих и возникающих угроз и того, как международное право, включая международное гуманитарное право и право прав человека, должно применяться к использованию государствами информационно-коммуникационных технологий. Разработка и осуществление мер укрепления доверия и механизмов практического

⁴ [A/78/265](#), приложение С.

сотрудничества между государствами также были отнесены к числу вопросов, требующих решения.

Создание, формат и принятие решений

26. Государства по-разному оценивали формат в плане создания будущего механизма, равно как и подготовительные усилия, предшествующие его созданию. Было выражено мнение о том, что основой для создания будущего механизма с точки зрения его сферы охвата, структуры и формата работы должны стать материалы, представленные государствами-членами в рамках нынешней рабочей группы открытого состава, включая предложение в отношении программы действий, доклад Генерального секретаря о такой программе действий, подготовленный в соответствии с резолюцией 77/37 Генеральной Ассамблеи⁵, настоящий доклад и соответствующие рекомендации, содержащиеся в докладах действующей рабочей группы открытого состава.

27. Многие государства подчеркнули важность достижения консенсуса в отношении сферы охвата, структуры и формата работы будущего механизма. Многие государства высказались за дальнейшую разработку и развитие этого механизма в рамках нынешней рабочей группы открытого состава. Несколько государств поддержали идею проведения в рамках действующей рабочей группы открытого состава дальнейших целенаправленных обсуждений в целях разработки механизма и поиска консенсуса относительно его формата и структуры. Что касается программы действий, то несколько государств поддержали идею проведения в 2024 и 2025 годах специальных межсессионных совещаний по этому предложению для дальнейшей проработки аспектов этого механизма. Также было предложено продолжить обсуждение последствий создания этого механизма для бюджета.

28. Была отмечена возможность налаживания в будущем регулярного институционального диалога на основе принятия консенсусом резолюции Генеральной Ассамблеи. В этой связи было высказано мнение, что резолюцией Ассамблеи должна быть учреждена постоянная рабочая группа открытого состава. Было также высказано мнение, что нынешняя рабочая группа открытого состава могла бы создать будущий механизм посредством политической декларации, которая впоследствии будет одобрена Генеральной Ассамблеей. Было выдвинуто предложение о том, что одним из ключевых элементов такой политической декларации могло бы стать подтверждение обязательства государств руководствоваться рамками ответственного поведения государств.

29. Что касается конкретного предложения в отношении программы действий, то несколько государств высказались в поддержку ее учреждения посредством принятия политической декларации. Было предложено дополнить декларацию резолюцией Первого комитета с описанием задач, структуры и формата программы действий. Также было предложено создать не позднее 2026 года международную конференцию для разработки и принятия такой декларации. Было высказано мнение о том, что если нынешняя рабочая группа открытого состава не сможет достичь консенсуса по заключительному докладу, включая соглашение о механизме, то для обеспечения непрерывности этих важных многосторонних обсуждений потребуются через Генеральную Ассамблею учредить международную конференцию или другую подготовительную процедуру, более универсальную по своему характеру.

⁵ A/78/76.

Механизм последующей деятельности и осуществление

30. Государства внесли различные предложения относительно механизма последующей деятельности, в том числе предложения относительно проведения регулярных совещаний, включая пленарные заседания и обзорные конференции, а также межсессионных заседаний, в том числе заседаний технических рабочих групп. Также было предложено проводить ежегодные официальные заседания механизма. Предложения в отношении периодичности проведения пленарных заседаний варьировались от одного раза в два года до одного раза в три года. Было высказано мнение, что для осуществления своей согласованной программы работы будущий механизм должен созывать совещания раз в два года. Было также высказано мнение о том, что, возможно, целесообразно было бы периодически проводить обзор работы постоянного механизма с целью убедиться, что применяемые им подходы соответствуют динамике оперативной обстановки в плане угроз.

31. Ряд государств поддержали идею создания технических рабочих групп, которые будут заниматься конкретными приоритетными вопросами, такими как применимость международного права и разработка новых норм, правил и принципов, а также, в соответствующих случаях, юридически обязывающих договоренностей. Было высказано мнение, что технические рабочие группы составят основу механизма, ориентированного на конкретные действия. Вспомогательным подгруппам было предложено рассмотреть конкретные аспекты мандата механизма. Прозвучало мнение, что заседания технических рабочих групп по конкретным вопросам в межсессионный период следует проводить в смешанном формате, с тем чтобы способствовать широкому участию государств. Было отмечено, что заседания подгрупп не следует проводить параллельно, чтобы делегации имели возможность полноценно принимать участие в работе всех подгрупп. Для содействия широкому участию государств было предложено учредить программу стипендий.

32. Государства высказали различные точки зрения относительно периодичности проведения возможных обзорных конференций, в том числе предложили проводить их раз в три или четыре года либо раз в шесть лет. Некоторые государства отметили, что на таких обзорных конференциях следует пересматривать рамки ответственного поведения государств в целях их обновления, при необходимости, и определения стратегического направления работы механизма. Было высказано мнение, что в ходе обзорных конференций целесообразно рассматривать вопрос о том, следует ли разрабатывать дополнительные нормы, правила, принципы или имеющие обязательную силу договоренности на основе консенсуса.

33. Многие государства говорили о важности того, чтобы принимать решения в рамках будущего механизма консенсусом. Ряд государств особо отметили, что решения по вопросам существа должны в обязательном порядке приниматься на основе консенсуса. По мнению нескольких государств, принцип, предусматривающий, что только государства могут принимать решения консенсусом, должен быть четко прописан в документе об учреждении будущего механизма. Государства высказали разные предложения относительно того, каким образом обеспечить сведение решений государств воедино в рамках будущего механизма, в том числе — в форме докладов о ходе работы, представляемых Генеральной Ассамблее на двухгодичной основе, а также в форме ежегодных процедурных докладов, сопровождаемых соответствующими решениями, принятыми на основе консенсуса.

34. Некоторые государства отметили возможность добровольного представления национальных докладов в рамках будущего механизма. Было предложено

представлять доклады об осуществлении нормативной базы на национальном уровне, а также доклады о национальной практике. Поступило предложение задействовать существующие инструменты, такие как национальный обзор выполнения рекомендаций Организации Объединенных Наций по ответственному использованию государствами информационно-коммуникационных технологий в контексте международной безопасности и Организации Объединенных Наций⁶.

35. Несколько государств отметили, что, хотя принятие решений останется исключительной прерогативой государств, взаимодействие с региональными и субрегиональными организациями может быть полезным, в том числе с точки зрения обеспечения синергетического эффекта и возможности действовать с опорой на существующие структуры и платформы, призванные способствовать наращиванию потенциала. Было предложено проводить межсессионные встречи с представителями таких организаций на ежегодной основе на основе консультаций с группами стран и соответствующим председателем будущего механизма. Кроме того, было предложено проводить обмен передовым опытом на международном, межрегиональном и региональном уровнях.

36. Государства придерживались разных позиций по вопросу о взаимодействии с неправительственными организациями в рамках будущего механизма, ссылаясь в качестве примера на формат участия в работе других форумов Организации Объединенных Наций, таких как Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях и Рабочая группа открытого состава по проблемам старения. Многие государства отметили, что большое значение для будущего функционирования механизма имеет участие многих заинтересованных сторон. Было отмечено, что максимально широкое участие заинтересованных сторон в будущем регулярном институциональном диалоге будет способствовать достижению общей цели поддержания мира и безопасности в сфере информационно-коммуникационных технологий и позволило бы приобрести ценный опыт по таким вопросам, как оценка угроз и применение норм. Ряд государств поддержали идею участия неправительственных организаций в соответствии с форматом, согласованным в рамках нынешней рабочей группы открытого состава. Несколько государств поддержали идею официального участия заинтересованных сторон и регулярных консультаций с ними, тогда как другие заявили, что взаимодействие с негосударственными субъектами должно носить исключительно консультативный и неофициальный характер, например, в рамках ежегодных межсессионных совещаний.

37. По мнению некоторых государств, подходящей структурой для выполнения функций секретариата будущего механизма является Управление по вопросам разоружения.

IV. Замечания и выводы Генерального секретаря

38. Обеспечение мира и безопасности в сфере информационно-коммуникационных технологий остается неотложной задачей. Одновременно с ростом обеспокоенности международного сообщества по поводу злонамеренного использования этих технологий различными субъектами цифровой разрыв увеличивается и быстро приближается срок достижения целей в области устойчивого развития. Требуется незамедлительно принять конкретные меры для предотвращения

⁶ <https://nationalcybersurvey.cyberpolicyportal.org>.

распространения и дальнейшей эскалации конфликта на эту область, в том числе для защиты жизни людей от злонамеренной деятельности.

39. Перед международным сообществом стоят серьезнейшие задачи по поддержанию мира и стабильности в сфере информационно-коммуникационных технологий, но при этом существует и прочный фундамент, на котором можно строить соответствующую деятельность. За более чем два десятилетия в рамках процессов под эгидой Генеральной Ассамблеи государства добились очень важного прогресса в выявлении существующих и возникающих угроз, определении применимости международного права к использованию государствами информационно-коммуникационных технологий, разработке рамок ответственного поведения государств при использовании этих технологий, а также в рассмотрении мер по укреплению доверия и инициатив в целях наращивания потенциала. Этот совокупный и последовательный прогресс был достигнут на основе консенсусных договоренностей. Тем самым была заложена прочная основа для дальнейшего прогресса.

40. Усилия, которые государства прилагают в рамках текущей деятельности рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, свидетельствуют о потенциальных возможностях принятия дальнейших конкретных мер по достижению общих целей создания мирной и безопасной информационно-коммуникационной среды. Последовательный прогресс в рамках данного форума свидетельствует о том, что при наличии достаточной политической воли можно не только достигать общих договоренностей, но можно и предпринимать практические действия. В этой связи я приветствую достигнутую государствами консенсусную договоренность о создании глобального межправительственного реестра контактных пунктов в целях укрепления взаимодействия и сотрудничества между ними. Это значимый шаг, способствующий укреплению международного мира и безопасности, повышению прозрачности и предсказуемости.

41. На этом фоне государства признали исключительную важность поддержания регулярного институционального диалога по таким вопросам, с тем чтобы обеспечить достаточное пространство для достижения неуклонного прогресса. Ожидается, что актуальность этих вопросов будет лишь возрастать по мере того, как такие технологии будут распространяться все более широко и будут занимать все большее место в нашей повседневной жизни.

42. Все государства согласны с тем, что такой регулярный институциональный диалог лучше всего проводить под эгидой Организации Объединенных Наций, которая обеспечивает максимально инклюзивную платформу для таких обсуждений. Также, согласно общему мнению, такой диалог направлен на поддержку целей укрепления международного мира, стабильности и предотвращения конфликтов в информационно-коммуникационной среде. Государства также подтверждают ряд важнейших принципов, которые составят основу такого диалога, например, таких как инклюзивность, прозрачность и ориентированность на конкретные действия. Кроме того, существует общее понимание необходимости создания одновекторного механизма, способствующего максимально широкому участию государств.

43. Если исходить из этих широких договоренностей и общих позиций, то достижение консенсуса в отношении будущего регулярного институционального диалога по информационно-коммуникационным технологиям в контексте международной безопасности представляется вполне выполнимой задачей. Государства имеют прекрасную возможность, опираясь на уже достигнутые успехи, найти в контексте деятельности нынешней рабочей группы открытого состава точки соприкосновения по вопросу о создании под эгидой Организации Объ-

единенных Наций одновекторного постоянного механизма, который будет функционировать на открытой, инклюзивной и прозрачной основе. Логичной и полезной отправной точкой в этом плане послужат общие элементы будущего регулярного институционального диалога, которые были согласованы на основе консенсуса и изложены в ежегодном докладе рабочей группы открытого состава о проделанной работе за 2023 год. Такие вопросы слишком важны, чтобы не воспользоваться этой возможностью для укрепления доверия. Постоянный механизм под эгидой Организации Объединенных Наций представляет собой следующий логический этап рассмотрения этих вопросов с участием многих сторон, в рамках которого будет учитываться прошлый опыт успешной деятельности и будут заложены основы для достижения прогресса в будущем.

Приложение

Ответы, полученные от правительств

Австралия

[Подлинный текст на английском языке]
[1 мая 2024 года]

Австралия приветствует возможность в ответ на предложение, содержащееся в резолюции 78/237 Генеральной Ассамблеи, изложить свои соображения относительно поощрения ответственного поведения государств в киберпространстве в контексте международной безопасности и будущего регулярного институционального диалога.

Настоящий документ основывается на материалах, представленных Австралией в ответ на резолюции 77/37 в 2023 году, 76/19 в 2022 году, 75/32 в 2021 году, 74/28 в 2020 году, 70/237 в 2016 году, 68/243 в 2014 году и 65/41 в 2011 году, посвященные достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Стратегия обеспечения кибербезопасности Австралии на 2023–2030 годы

22 ноября 2023 года министр кибербезопасности Клэр О’Нил представила Стратегию обеспечения кибербезопасности Австралии на 2023–2030 годы, в которой изложено видение Австралии относительно обеспечения внутренней и международной кибербезопасности на основе общегосударственного подхода к развитию потенциала противодействия киберугрозам.

В Стратегии выделены шесть аспектов для создания более надежной киберзащиты и быстрого восстановления после киберинцидентов: а) высокий потенциал развития предприятий и сильное гражданское общество; б) безопасность технологий; с) совместное отражение и блокирование угроз всемирного масштаба; d) защита объектов критически важной инфраструктуры; e) суверенные возможности; и f) надежное региональное и глобальное руководство.

В Стратегии зафиксирована неизменная приверженность Австралии формированию, поддержанию и защите международных правил, норм и стандартов в сфере обеспечения кибербезопасности, в том числе путем соблюдения международного права и норм ответственного поведения государств в киберпространстве, а также использования всех возможностей государственного аппарата для пресечения действий злоумышленников и принятия соответствующих мер реагирования.

Соблюдение международного права и норм ответственного поведения государств в киберпространстве

Австралия будет сотрудничать с ее действующими партнерами и налаживать новые партнерские отношения в интересах соблюдения международного права и согласованных нормативных рамок ответственного поведения государств, которые лежат в основе нашей стабильности, процветания, независимости и суверенитета в киберпространстве.

Все страны согласились использовать киберпространство в соответствии с правилами, основанными на действующем международном праве и международных нормах. Международное право, дополненное согласованными добровольными нормами ответственного поведения государств, мерами укрепления доверия и усилиями по наращиванию потенциала, обеспечивает надежную ос-

нову для предсказуемости и стабильности в киберпространстве. При их внедрении и соблюдении указанные нормативные рамки обеспечивают инструментарий для противодействия угрозам, возникающим в результате злонамеренной киберактивности государств и финансируемой ими киберактивности.

Австралия будет взаимодействовать со своими международными партнерами в рамках дискуссий в Организации Объединенных Наций, чтобы прояснить, как международное право применяется в киберпространстве, и активизировать процесс внедрения рамок ответственного поведения государств в киберпространстве. Подобные усилия будут охватывать укрепление сотрудничества в рамках региональных форумов, в том числе в рамках Форума тихоокеанских островов и на основе взаимодействия с Региональным форумом Ассоциации государств Юго-Восточной Азии.

Использование всех возможностей государственного аппарата для пресечения действий злоумышленников и принятия соответствующих мер реагирования

Австралия будет использовать все возможности государственного аппарата для пресечения действий злоумышленников в киберпространстве и принятия соответствующих мер реагирования. Австралия будет сотрудничать со своими международными партнерами, чтобы ввести меры наказания для отдельных лиц и организаций, которые делают киберпространство менее безопасным и менее защищенным. Это предполагает, в частности, выявление случаев, когда государства действуют в ущерб международному праву и международным нормам или нарушают их, а также введение санкций в отношении тех, кто совершает крупные киберинциденты или способствует их совершению, в тех случаях, когда у нас имеются достаточные доказательства и когда это отвечает нашим национальным интересам.

Во всех своих действиях Австралия будет придерживаться действующих норм международного права и согласованных добровольных норм ответственного поведения государств в киберпространстве.

Поддержка регионального потенциала противодействия киберугрозам

Австралия будет продолжать сотрудничать со своими соседями в Тихоокеанском регионе и Юго-Восточной Азии, чтобы укрепить региональный потенциал противодействия киберугрозам. Сотрудничество и помощь будут по-прежнему координироваться послом Австралии по вопросам киберпространства и важнейших технологий.

Австралия пересматривает направленность своих усилий по сотрудничеству и наращиванию потенциала в киберпространстве, с тем чтобы они были более целенаправленными, эффективными и устойчивыми и позволяли ее соседям успешнее предотвращать киберинциденты и быстро восстанавливаться в случае их совершения. Поскольку люди по-разному относятся к вопросам кибербезопасности, мы будем и далее учитывать в рамках наших усилий вопросы гендерного равенства, инвалидности и социальной инклюзии. Это предполагает постоянную поддержку повестки дня Организации Объединенных Наций по вопросу о женщинах и мире и безопасности, а также Национального плана действий Австралии по вопросу о женщинах и мире и безопасности на 2021–2031 годы.

Когда в регионе будут происходить серьезные киберинциденты, Австралия будет иметь больше возможностей для реагирования на просьбы о помощи. Австралия занимается формированием региональной группы по реагированию на киберкризисы при Министерстве иностранных дел и торговли, которая будет опираться на опыт специалистов из правительства, промышленности и техни-

ческого сообщества. В ответ на запросы правительств в связи с серьезными киберинцидентами в регионе эта группа будет помогать сдерживать масштабы и последствия киберинцидентов и восстанавливать критически важные сервисы и инфраструктуру.

Регулярный институциональный диалог

Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности

Австралия поддерживает создание единого, постоянного, гибкого, общедоступного, транспарентного и ориентированного на практические действия механизма под эгидой Первого комитета для обсуждения, имплементации и совершенствования нормативных рамок ответственного поведения государств в киберпространстве, согласованных и подтвержденных Генеральной Ассамблеей на основе консенсуса. Эти нормативные рамки базируются на международном праве, нормах и мерах укрепления доверия и поддерживаются скоординированными действиями по наращиванию потенциала. Программа действий должна служить форумом, на котором все 193 государства-члена смогут конструктивно участвовать как в обсуждении, так и в практических действиях на регулярной и постоянной основе. Программа действий должна предусматривать возможности для роста, перестройки и совершенствования — она должна способствовать внедрению существующих согласованных нормативных рамок и допускать возможность дальнейшей их оптимизации на основе консенсуса по мере возникновения новых угроз и вызовов.

В своей резолюции [77/37](#) Генеральная Ассамблея приветствовала предложение о разработке программы действий и просила Генерального секретаря запросить мнения государств-членов о сфере охвата, структуре и содержании программы действий. В соответствующем докладе ([A/78/76](#)) государствам было рекомендовано продолжать обсуждать сферу охвата, структуру, принципы, содержание, функции и последующий механизм предлагаемой программы действий под эгидой рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 с учетом мнений, изложенных в этом докладе, а также результатов региональных и субрегиональных консультаций, организованных Управлением по вопросам разоружения в соответствии с резолюцией [77/37](#) Генеральной Ассамблеи.

Рабочая группа открытого состава играет ключевую роль в разработке программы действий и связанной с ней подготовительной работе. Программа действий должна опираться на достигнутый с большим трудом консенсус и совокупность результатов дискуссий шести последних сменявших друг друга групп правительственных экспертов, а также первой и текущей рабочих групп открытого состава. Постоянный механизм представляет собой следующий этап или эволюцию в киберархитектуре Организации Объединенных Наций, которая основывается на предыдущем опыте и гарантирует, что в будущем этим вопросам будет уделяться внимание и придаваться значение, которых они заслуживают.

В своей резолюции [78/16](#) Генеральная Ассамблея постановила учредить по завершении деятельности рабочей группы открытого состава 2021–2025 и не позднее 2026 года механизм под эгидой Организации Объединенных Наций, который будет постоянным, инклюзивным и ориентированным на практические действия и который будет иметь конкретные цели, как это указано в резолюции [77/37](#) Генеральной Ассамблеи, и общие элементы для будущего регулярного институционального диалога, согласованные консенсусом в ежегодном докладе рабочей группы открытого состава 2021–2025 о проделанной работе за 2023 год.

Австралия поддерживает предложение о созыве в 2025 году международной конференции для принятия учредительного документа программы действий на основе подготовительной работы, проделанной рабочей группой открытого состава 2021–2025.

Австралия выступает за разработку учредительного документа для программы действий, в котором будут изложены обязательства государств и будет предусмотрен механизм, который может быть одобрен в резолюции Генеральной Ассамблеи. В учредительном документе, который может быть составлен в форме политической декларации, следует:

- одобрить и подтвердить политическую приверженность государств нормативным рамкам (включая применение действующего международного права в киберпространстве), согласованным в докладах групп правительственных экспертов¹ и в докладе рабочей группы открытого состава²;
- напомнить о существующих и возникающих угрозах международной безопасности, связанных со злонамеренным использованием информационно-коммуникационных технологий (ИКТ), основываясь на оценках угроз, содержащихся в докладах групп правительственных экспертов и рабочей группы открытого состава;
- предусмотреть учреждение постоянного институционального механизма для содействия имплементации этих нормативных рамок (включая поддержку потенциала государств в этом контексте) и соответствующие форматы его учреждения;
- обеспечить условия для дальнейшего совершенствования и обновления нормативных рамок, по мере необходимости, для включения в них консенсусных принципов, рекомендаций и обязательств в случае одобрения Генеральной Ассамблеей на основе консенсуса доклада рабочей группы открытого состава, Группы правительственных экспертов или других процессов Организации Объединенных Наций или в случае принятия на основе консенсуса соглашения на конференции по обзору программы действий;
- определить основные направления работы для программы действий на основе вопросов, которые международное сообщество согласно обсуждать и решать;
- прямо стимулировать и поощрять взаимодействие с соответствующими членами сообщества многих заинтересованных сторон в соответствующих областях.

Что касается правил процедуры, то Австралия вновь заявляет, что программа действий должна предусматривать согласование всех вопросов на основе консенсуса (включая доклады, рекомендации и декларации).

Для того чтобы мероприятия по линии программы действий были основаны на фактах и данных, особое внимание в ней следует уделять поддержке усилий по имплементации, в том числе с помощью конкретных, целенаправленных и скоординированных мер по наращиванию потенциала. Меры по целенаправленному наращиванию потенциала следует тщательно продумать в рамках программы действий. В целях содействия целенаправленному наращиванию потенциала с учетом потребностей и на основе фактологической базы в программу действий можно включить рекомендации для государств-членов периодически проводить опросы и представлять самоотчеты о внедрении ими нормативных

¹ См. A/65/201, A/68/98, A/70/174 и A/76/135.

² A/75/816.

рамок (например, раз в три года или в противном случае в соответствии с циклом проведения обзорных конференций), используя стандартизированный механизм отчетности — обзор хода реализации на национальном уровне рекомендаций Организации Объединенных Наций по ответственному использованию государствами ИКТ в контексте международной безопасности (см. <https://nationalcybersurvey.cyberpolicyportal.org/>).

Австралия признает важную роль сообщества с участием многих заинтересованных сторон, включая гражданское общество, частный сектор, научные круги и техническое сообщество, в содействии процессу формирования свободного, открытого, безопасного, стабильного, доступного и мирного киберпространства. Австралия предлагает предусмотреть в программе действий положение о проведении регулярных и институционализированных консультаций с соответствующими заинтересованными сторонами.

Резюмируя вышесказанное, Австралия подчеркивает, что программа действий должна иметь четкий мандат, опирающийся на согласованные нормативные рамки и подтверждающий их; быть гибкой — как в содержательном плане, поскольку нормативные рамки могут быть в дальнейшем доработаны на основе консенсуса, так и в процедурном плане; обеспечивать поддержку усилий по их имплементации с помощью добровольной отчетности и наращивания потенциала; и быть инклюзивной в том смысле, что решения по вопросам, связанным с международной безопасностью, остаются прерогативой государств, но обсуждения и рабочие группы открыты для участия сообщества многих заинтересованных сторон.

Австралия рассчитывает на продолжение сотрудничества с Генеральным секретарем, Управлением по вопросам разоружения и государствами-членами в усилиях по разработке эффективной, гибкой и инклюзивной программы действий.

Азербайджан

[Подлинный текст на английском языке]
[1 мая 2024 года]

За последние годы киберпространство существенно изменилось, что открывает перспективы для улучшения нашей повседневной жизни — от безопасности и защищенности до скорости коммуникации и использования цифровых технологий. Достижения в области кибертехнологий и важнейших технологий лежат в основе будущего процветания мира, но в то же время они способны подорвать стабильность и предсказуемость. Поэтому важно содействовать принятию мер по наращиванию потенциала и созданию надлежащих средств защиты и цифровых услуг, которые будут способствовать повышению безопасности киберпространства.

Усилия, прилагаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области

Азербайджан поддерживает деятельность рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, созданной в соответствии с резолюцией 75/240 Генеральной Ассамблеи. Будучи одним из соавторов резолюции 78/237 Ассамблеи, Азербайджан предпринял ряд шагов по укреплению своей информационной безопасности и развитию международного сотрудничества в области обеспечения кибербезопасности.

Следует отметить, что Стратегия Азербайджанской Республики по обеспечению информационной безопасности и кибербезопасности на 2023–2027 годы, утвержденная Указом Президента Азербайджанской Республики от 28 августа 2023 года, направлена на повышение уровня национальной информационной безопасности в интересах безопасного использования современных информационно-коммуникационных технологий (ИКТ) государством, обществом и отдельными лицами, предусматривает определение и осуществление мер по обеспечению безопасности государства, частных сетей и критически важной информационной инфраструктуры и защите персональных данных и способствует тем самым созданию более благоприятных условий для реализации прав и свобод человека, закрепленных в Конституции Азербайджанской Республики. Будучи первой стратегией Азербайджанской Республики в сфере информационной безопасности и кибербезопасности, она является неотъемлемым компонентом государственной политики в области ИКТ и определяет ее основные цели, направления, приоритетные задачи, соответствующие решения и план комплексных мер, регулирующих эту область.

Кроме того, в разделе 8.9.2.3. Плана действий Стратегии отмечаются «постоянные усилия по содействию расширению международного сотрудничества и изучению международного опыта в области обеспечения кибербезопасности на уровне субъектов информационной безопасности, включая Национальную группу реагирования на компьютерные инциденты и другие группы реагирования на компьютерные инциденты», при этом основной целью является развитие сотрудничества с международными центрами групп реагирования на компьютерные инциденты и обеспечение членства в международных центрах групп реагирования на компьютерные инциденты. В настоящее время ведется практическая работа, направленная на расширение совместной деятельности и обмен опытом.

Стоит отметить, что Правила обеспечения безопасности критически важной информационной инфраструктуры в Азербайджанской Республике и Правила по структурированию, созданию и ведению реестра объектов критически важной информационной инфраструктуры были утверждены соответствующими решениями Кабинета министров Азербайджанской Республики в 2023 году.

Кроме того, в результате совместных действий Службы государственной безопасности Азербайджанской Республики и Ассоциации организаций кибербезопасности Азербайджана позиция страны в международной рейтинговой таблице Индекса национальной кибербезопасности в 2023 году сместилась с семьдесят шестого на пятидесятое место.

Государственная служба специальной связи и информационной безопасности Азербайджанской Республики разработала проект руководства по обеспечению информационной безопасности, который будет представлен государственным органам в целях обеспечения информационной безопасности в государственных учреждениях, включая информацию о превентивных и корректирующих мерах против потенциальных угроз в корпоративной информационной среде.

Для укрепления потенциала противодействия киберугрозам и повышения осведомленности в этой области сотрудников государственных учреждений, а также представителей частного сектора и владельцев предприятий был реализован проект в области кибергигиены.

26 и 27 октября 2023 года состоялся киберфестиваль «Оборона объектов критически важной инфраструктуры — 2023», организованный совместно Государственной службой специальной связи и информационной безопасности и Службой государственной безопасности и направленный на расширение опыта, знаний и навыков представителей местных и зарубежных компаний и

государственных и частных учреждений, работающих в сфере кибербезопасности, критически важной инфраструктуры, финансового и телекоммуникационного секторов.

На Международной конференции по кибердипломатии, проведенной Национальным институтом исследований и разработок в области информатики в апреле 2023 года в Румынии, было решено, что в 2024 году Азербайджан станет принимающей страной следующей конференции.

В результате практических мероприятий, проводимых с целью формирования и развития национальной экосистемы в области обеспечения кибербезопасности, позиции Азербайджана в международных рейтингах значительно улучшились. Согласно Глобальному индексу кибербезопасности Международного союза электросвязи за 2020 год Азербайджан улучшил свою позицию на 15 пунктов, заняв сороковое место среди 194 стран с результатом 89,31 балла.

Что касается международного сотрудничества в указанной области, то представители различных ведомств Азербайджанской Республики принимают участие в международных мероприятиях, посвященных сотрудничеству в борьбе с киберугрозами, обмену информацией и опытом в связи с инцидентами в сфере кибербезопасности и разработке политики и стратегии в области кибербезопасности. К таким мероприятиям относятся заседания межправительственного Специального комитета открытого состава по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, а также мероприятия в рамках проектов «КиберВосток», Агентства Европейского союза по подготовке сотрудников правоохранительных органов и Учебно-оперативного партнерства по борьбе с организованной преступностью, совместно финансируемых Европейским союзом и Советом Европы.

Канада

[Подлинный текст на английском языке]
[16 апреля 2024 года]

Тенденция роста злонамеренной активности в киберпространстве в последние годы побуждает к принятию эффективных мер по смягчению угроз, которые могут потенциально подорвать международную безопасность и стабильность.

Потребность в расширении сотрудничества и практических усилий должна сопровождаться созданием соответствующего механизма Организации Объединенных Наций по обеспечению кибербезопасности. Канада подчеркивает необходимость опираться на коллективную нормативную базу (действующие нормы и наше общее понимание того, как применяется международное право) и создать пространство для проведения более глубоких, конкретных и технических обсуждений, которые будут неразрывно связаны с нашими дискуссиями на пленарных заседаниях. Канада считает, что будущий регулярный институциональный диалог должен функционировать как непрерывный цикл, включающий в себя оценку угроз, обсуждение хода внедрения нормативных рамок, укрепление потенциала и обзор всех выявленных недостатков, которые необходимо устранить. Работа над реальными проблемами или над сценариями, моделирующими такие проблемы, с большей вероятностью прольет свет на практические решения по смягчению последствий. Будущий регулярный институциональный диалог должен быть ориентирован на конкретные действия и результаты и должен демонстрировать устойчивый и поддающийся измерению прогресс.

Будучи владельцами и операторами инфраструктуры в киберпространстве, а также нашими «глазами и ушами» на местах, сообщество многих заинтересованных сторон имеет все возможности для внесения высококачественного и уникального вклада в нашу работу на консультативной основе. Обеспечение значимого участия заинтересованных сторон в будущем регулярном институциональном диалоге будет играть важную роль в достижении нашей общей цели — поддержании киберстабильности. Привлечение таким образом сообщества многих заинтересованных сторон также является наиболее перспективным подходом к расширению возможностей для приобщения малых и развивающихся государств к нашей работе. Это, в свою очередь, создаст возможности для максимального укрепления глобального потенциала противодействия киберугрозам в интересах всех и каждого. Будучи по-настоящему инклюзивным, будущий регулярный институциональный диалог имеет больший потенциал для получения поддержки, которая может обеспечить добросовестную имплементацию и формирование ответственного поведения государств в киберпространстве.

Тревоги и интересы всех государств, в том числе в отношении дальнейшего развития нормативных рамок, необходимо будет учесть в ходе будущего регулярного институционального диалога на основе равного участия государств в работе Организации Объединенных Наций. Решения по вопросам существа следует принимать на основе консенсуса.

Канада ссылается на высказанные ею мнения относительно будущего регулярного институционального диалога в контексте доклада Генерального секретаря о программе действий в соответствии с резолюцией [77/37](#) Генеральной Ассамблеи от апреля 2023 года и подтверждает их. В этих мнениях отражено, в частности, то, что Канада признает и приветствует доклады и рекомендации, принятые на сегодняшний день консенсусом (например, выпущенные в 2021 году доклады Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и Рабочей группы открытого состава достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности). Канада считает, что наиболее оптимальным вариантом действий этой рабочей группы открытого состава для выполнения ее мандата, предусмотренного резолюцией [75/240](#) Генеральной Ассамблеи, является принятие решения о проведении одновекторного, постоянного, ориентированного на конкретные действия и инклюзивного регулярного институционального диалога.

Канада приветствует возможность вновь высказать свои соображения относительно будущего регулярного институционального диалога. Канада считает, что нынешний механизм рабочей группы открытого состава не является оптимальным или достаточным для достижения наших коллективных целей. Канада не поддержит повторение или постоянное продление нынешнего механизма рабочей группы открытого состава. Напротив, Канада твердо убеждена, что программа действий, разработанная в рамках рабочей группы открытого состава и, в идеале, согласованная на основе консенсуса, является наилучшим вариантом для проведения одновекторного, постоянного, ориентированного на конкретные действия и инклюзивного регулярного институционального диалога по вопросам кибербезопасности. Этот процесс позволит более целенаправленно добиваться внедрения норм и более подробно обсуждать вопрос о том, как применяется международное право. Это также обеспечит более эффективную и ориентированную на конкретные действия координацию (в рамках нынешней рабочей группы открытого состава такая координация отсутствует) между обсуждением конкретной реализации нормативных положений и целенаправленным наращиванием потенциала.

Канада напоминает, что предметные обсуждения программы действий в рамках будущего регулярного институционального диалога проводятся с 2021 года, в том числе в контексте рабочего документа, распространенного в рамках этой рабочей группы открытого состава¹. Канада признает и поддерживает призывы других государств-членов к организации одновекторного процесса обсуждения вопросов кибербезопасности в Организации Объединенных Наций. В связи с этим Канада предостерегает от создания отдельного параллельного процесса для регулярного институционального диалога, который будет конкурировать с программой действий, получившей поддержку 161 государства-члена в резолюции 78/16 Генеральной Ассамблеи. Это будет неоправданным и ненужным дублированием усилий и приведет к лишним трудовым и финансовым затратам государств-членов.

Структура и функционирование программы действий будут определены на международной конференции, на которой будет принята политическая декларация. Предполагается, что программа действий будет обслуживаться Управлением по вопросам разоружения, который будет выступать в качестве секретариата. Будут проводиться обзорные конференции для выработки стратегического ориентира, пленарные дискуссии открытого состава, аналогичные тем, что проводятся в рамках нынешнего механизма рабочей группы открытого состава, и технические совещания или рабочие группы для координации элементов тематических дискуссий, имеющих отношение к борьбе с конкретными угрозами (например, определение мероприятий по наращиванию потенциала, наиболее значимых для внедрения норм и применения международного права в отношении вирусов-вымогателей).

В рамках программы действий будет предусмотрено инвестирование в наращивание потенциала и оказание технической помощи в качестве важнейших компонентов для дальнейшего обеспечения ответственного поведения государств в киберпространстве и содействия сотрудничеству между государствами. Она позволит налаживать региональное взаимодействие через сотрудничество с региональными организациями, чтобы стимулировать взаимодействие и координировать инициативы.

Программа действий не ограничится выпуском докладов председателя. Кроме того, она должна будет демонстрировать стабильный и поддающийся измерению прогресс. Она будет направлена на устранение пробела в плане подотчетности между нормативной базой и реальной практикой путем закрепления обязательств и внедрения механизмов отчетности или обзора, с тем чтобы способствовать осуществлению оптимальной деятельности по наращиванию потенциала в целях обеспечения более ответственного поведения государств во всем мире.

Китай

[Подлинный текст на китайском языке]
[29 апреля 2024 года]

Мнение правительства Китая в отношении будущего постоянного механизма поддержания институционального диалога.

Правительство Китая, ссылаясь на резолюцию 78/237 Генеральной Ассамблеи о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, излагает следующую позицию и мнение в отно-

¹ См. <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

шении будущего постоянного механизма поддержания институционального диалога.

Вопрос о будущем постоянном механизме имеет огромное значение для того, как Организация Объединенных Наций будет подходить к вопросам информационной безопасности. Китай поддерживает создание в рамках Организации Объединенных Наций единого будущего постоянного механизма поддержания институционального диалога по вопросам кибербезопасности, характеризующегося всеобщим участием. Единственным возможным вариантом для всех сторон является достижение консенсуса по вопросу о будущем постоянном механизме в рамках Рабочей группы открытого состава. Китай не поддерживает какие-либо попытки создать постоянный механизм за рамками Рабочей группы. Мы против того, чтобы начинать эту работу с нуля, поскольку это приведет к раздробленности процессов Организации Объединенных Наций в области информационной безопасности и возникновению геополитических разногласий и конфронтации между блоками. Такое развитие событий не отвечает интересам ни одного из государств-членов.

Что касается структуры и функций будущего постоянного механизма, то он должен закрепить важные результаты, достигнутые в поддержании процессов Организации Объединенных Наций в области информационной безопасности за последние 26 лет, и отвечать целям долгосрочного развития. Его структура может состоять из двух компонентов: первый будет основан на анализе прошлого и посвящен соблюдению и реализации существующих рамок ответственного поведения государств в киберпространстве, особенно в целях обогащения и улучшения планов действий по наращиванию потенциала. Второй компонент будет ориентирован на перспективу и направлен на то, чтобы идти в ногу со временем, формулировать новые стандарты, в том числе в области безопасности данных, содействовать разработке соответствующего правового документа и предлагать новые планы действий по наращиванию потенциала. Китай представил Глобальную инициативу по безопасности данных с целью предложить практические решения проблем в области безопасности данных. Согласно этой инициативе страны не должны требовать от своих компаний хранить на своей территории данные, сгенерированные или полученные за рубежом; они должны уважать суверенитет, юрисдикцию и право других стран на управление безопасностью данных и не должны напрямую получать доступ к данным компаний или частных лиц в других странах без законного разрешения этих стран. В рамках этой инициативы были выдвинуты конкретные предложения по защите объектов критически важной инфраструктуры и обеспечению безопасности цепочек поставок. Информация об этой инициативе была распространена в качестве официального документа Генеральной Ассамблеи Организации Объединенных Наций. Китай готов сотрудничать со всеми сторонами с целью способствовать разработке международных правил регулирования цифровой среды, которые отражали бы пожелания и учитывали интересы всех сторон.

Будущий постоянный механизм должен возглавляться государствами-членами и в то же время обеспечивать участие различных заинтересованных сторон, как это происходит в Рабочей группе открытого состава. Каждые пять лет можно проводить обзорные конференции, а ежегодно — два или три пленарных заседания. В течение первых трех лет цикла обзора можно проводить целенаправленные предметные обсуждения и на основе консенсуса принимать ежегодные доклады и решения по важным вопросам, представляющим широкий интерес для государств-членов. В четвертый год цикла обзора можно начать процесс подготовки к обзорной конференции и под именем Председателя разработать сводные документы. В течение пятого года цикла обзора можно провести предметные обсуждения, главным образом на основе сводных документов

Председателя, достичь, возможно путем переговоров, существенного консенсуса и составить план работы на следующие пять лет.

Китай готов и впредь активно участвовать в соответствующем процессе и вносить свой вклад в создание будущего постоянного механизма.

Китай надеется, что изложенные им мнения найдут отражение в соответствующих докладах Генерального секретаря Организации Объединенных Наций.

Куба

[Подлинный текст на испанском языке]
[29 апреля 2024 года]

Достижения в области информационно-коммуникационных технологий всё сильнее влияют на все сферы жизни общества. Нельзя допускать, чтобы этот прогресс сказался на безопасности государств.

Куба подтверждает, что информационно-коммуникационные технологии должны использоваться в мирных целях и что государства должны вести себя ответственно в интересах общего блага человечества, чтобы способствовать устойчивому развитию всех стран.

Мы подтверждаем, что предотвратить превращение киберпространства в театр военных действий можно только на основе сотрудничества всех государств.

Необходимо, чтобы Генеральная Ассамблея Организации Объединенных Наций безотлагательно приняла юридически обязывающий международный документ, который дополнит применимое международное право, устранил серьезные юридические пробелы в сфере кибербезопасности и позволит эффективно реагировать на растущие вызовы и угрозы, с которыми мы сталкиваемся.

Подходящей площадкой для достижения этой цели является рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Отводимую этой группе роль в проведении регулярного институционального диалога по вопросам безопасности и использования информационно-коммуникационных технологий необходимо уважать и поддерживать. Мы выступаем за сохранение нынешнего формата работы этой группы, с тем чтобы она могла достичь основанных на консенсусе результатов в интересах всех государств.

Все государства должны соблюдать существующие международные стандарты в этой области. Доступ к информационно-телекоммуникационным системам другого государства должен предоставляться в соответствии с достигнутыми соглашениями о международном сотрудничестве на основе принципа согласия соответствующего государства. При определении формата и масштабов обмена должно соблюдаться законодательство того государства, к системе которого предоставляется доступ.

Использование телекоммуникаций во враждебных целях с явным или тайным намерением подорвать правовые и политические системы государств является нарушением соответствующих признанных на международном уровне норм и представляет собой незаконное и безответственное использование этих средств.

С помощью незаконных радио- и телепередач совершаются постоянные вторжения в информационное пространство Кубы, а также распространяются программы, специально предназначенные для подстрекательства к свержению конституционного строя, установленного кубинским народом.

На протяжении 2023 года с территории Соединенных Штатов велось незаконное вещание на Кубу в среднем в течение 7000 часов в неделю на 21 частоте, что идет вразрез с целями и принципами, закрепленными в Уставе Организации Объединенных Наций, нормами международного права и положениями Международного союза электросвязи.

Экономическая, торговая и финансовая блокада, введенная правительством Соединенных Штатов в отношении Кубы более 60 лет назад, наносит серьезный ущерб кубинскому народу, в том числе в плане использования информационно-телекоммуникационных технологий.

Мы вновь выступаем против введения односторонних принудительных мер, которые противоречат нормам международного права и препятствуют оказанию помощи, сотрудничеству и передаче технологий.

В нашем регионе признается потенциал информационно-коммуникационных технологий для поиска новых решений проблем развития и содействия устойчивому, инклюзивному и справедливому экономическому росту, а также осуществления Повестки дня в области устойчивого развития на период до 2030 года.

Кроме того, следует особо отметить необходимость содействия созданию открытой, безопасной, стабильной, доступной и мирной среды в сфере ИКТ, о чем говорится в декларации восьмого Саммита Сообщества государств Латинской Америки и Карибского бассейна, который прошел в 2024 году в Кингстауне.

Куба вновь заявляет, что международное сотрудничество имеет основополагающее значение для противостояния угрозам, связанным с неправомерным использованием информационно-коммуникационных технологий.

Чехия

[Подлинный текст на английском языке]
[30 апреля 2024 года]

Чехия всецело привержена продвижению глобальных прений по вопросу о кибербезопасности в Организации Объединенных Наций и благодарна за прогресс, достигнутый к настоящему времени как рабочими группами открытого состава, так и группами правительственных экспертов.

Одним из главных достижений рабочей группы открытого состава и Группы правительственных экспертов является разработка и закрепление нормативных рамок ответственного поведения государств в киберпространстве.

В этом контексте Чехия считает, что внедрение рамок ответственного поведения государств в киберпространстве должно стать центральной темой будущего институционального диалога. Кроме того, Чехия поддерживает идею создания — по завершении работы нынешней рабочей группы открытого состава в 2025 году — постоянного, одновекторного, инклюзивного и ориентированного на конкретные действия механизма под эгидой Организации Объединенных Наций.

В то же время мы считаем, что для налаживания будущего институционального диалога, который будет эффективно работать на благо всех нас, важно

продолжить обсуждение его конкретной формы в рамках нынешней рабочей группы открытого состава. В настоящее время у нас как членов международного сообщества осталось чуть больше года, чтобы провести эти обсуждения.

Что касается обсуждений в рамках рабочей группы открытого состава, то Чехия хотела бы обратить ваше внимание на то, что наиболее проработанным, обсуждаемым и согласованным предложением относительно формы будущего институционального диалога является программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ).

Вместе с тем мы считаем, что резолюция [78/237](#) о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности не опирается на поэтапный подход и консенсус, который был достигнут в рамках рабочей группы открытого состава в последние годы. Нам кажется, что приоритет в ней отдается интересам узкой группы государств.

Обсуждения программы действий ведутся непрерывно с 2020 года, и Чехия принимает в них активное участие. Мы признаем ценность продолжающегося обсуждения программы действий в рамках рабочей группы открытого состава для определения направленности программы действий и прояснения ряда потенциально спорных моментов. Мы считаем, что важно продолжить эти обсуждения, чтобы определить содержание и формат работы будущего механизма. В свете вышесказанного мы предлагаем организовать межсессионные заседания и специальные сессии рабочей группы открытого состава в 2024 и 2025 годах, чтобы уделить внимание конкретным аспектам программы действий, включая последствия для бюджета.

Кроме того, Чехия хотела бы обратить внимание на некоторые аспекты программы действий, которые возникли в ходе обсуждения программы действий и которые Чехия считает наиболее значимыми преимуществами программы действий:

- программа действий позволит обеспечить институциональную стабильность при проведении международных дискуссий по ИКТ. Она будет служить постоянной институциональной основой для всех обсуждений по проблематике киберпространства в рамках Организации Объединенных Наций. Это позволит избежать необходимости периодического обсуждения вопроса о создании новой рабочей группы, посвященной вопросам использования ИКТ;
- программа действий будет способствовать внедрению нормативных рамок ответственного поведения государств и позволит, при необходимости, продолжить обсуждение их разработки;
- программа действий будет направлена на практическое применение принципов укрепления потенциала в рамках ее ориентированных на конкретные действия целей и на содействие их реализации в рамках проектов по наращиванию потенциала в области обеспечения кибербезопасности. В перспективе это может способствовать активизации текущих и потенциальных усилий по наращиванию потенциала, повышению их наглядности и улучшению координации таких усилий. В частности, было бы полезно изучить возможность координации усилий с мероприятиями по наращиванию киберпотенциала, проводимыми на других площадках, таких как Международный союз электросвязи;
- программа действий будет способствовать конструктивному участию неправительственных заинтересованных сторон и сотрудничеству с ними.

Участие частного сектора, научных кругов и гражданского общества позволит приобрести ценный опыт по таким вопросам, как оценка угроз и внедрение норм, включая оценку достигнутого прогресса;

- программа действий призвана служить всеобъемлющей основой, потенциально охватывающей другие инициативы, которые обсуждались или были согласованы в рамках рабочей группы открытого состава.

Что касается конкретных форматов работы, то Чехия поддерживает идею проведения ежегодных пленарных заседаний и заседаний специализированных технических рабочих групп в межсессионный период.

- Вопрос о создании и прекращении деятельности конкретной рабочей группы будет относиться исключительно к компетенции государств.
- Сфера охвата вышеупомянутых технических дискуссий и связанная с ними подготовительная работа будут ограничены темами, определенными на пленарных заседаниях. В дискуссиях будет участвовать, например, ограниченное число экспертов из правительств и, когда это уместно, других заинтересованных сторон, таких как научные круги. В частности, такие рабочие группы могут заниматься такими темами, как защита критически важной инфраструктуры, реагирование на киберинциденты и применимость конкретных положений по конкретным вопросам в рамках международного права к киберпространству.
- Если все будет организовано правильно, мы считаем, что наличие межсессионных технических рабочих групп может значительно повысить эффективность нашей работы и снизить нагрузку на отдельные делегации.
- Возможно, будет полезно рассмотреть возможность проведения в Нью-Йорке не всех межсессионных заседаний рабочих групп, а обсудить возможность проведения заседаний и в других местах.

Дания

[Подлинный текст на английском языке]
[1 мая 2024 года]

Дания считает, что внедрение принятых Организацией Объединенных Наций нормативных рамок ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ) имеет ключевое значение для обеспечения глобального, открытого, стабильного и безопасного киберпространства. Международное сообщество признает, что действующее международное право и Устав Организации Объединенных Наций в полном объеме применимы к сфере ИКТ, и Дания по-прежнему привержена внедрению этих нормативных рамок в отношении киберпространства.

За прошедшие 20 лет был достигнут значительный прогресс в разработке консолидированных рамок ответственного поведения государств в киберпространстве, включая применение международного права и добровольных норм и принятие мер по наращиванию потенциала и укреплению доверия. Эти рамки неоднократно утверждались Генеральной Ассамблеей на основе консенсуса, в последний раз — в консенсусном ежегодном докладе о проделанной работе за 2023 год, представленном рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Дания, как и Европейский союз, считает, что некоторые части резолюции [78/237](#) о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности, принятой Генеральной Ассамблеей

22 декабря 2023 года, основаны на тексте, не пользующемся консенсусной поддержкой. В частности, шестнадцатый пункт преамбулы и пункт 5 постановляющей части основаны на предложениях, поддерживаемых лишь ограниченной группой государств. Дания обеспокоена тем, что это может привести к новому толкованию существующих консенсусных документов. В связи с этим Дания не смогла поддержать резолюцию [78/237](#).

К вопросу о просьбе в соответствии с пунктом 8 постановляющей части резолюции

Организация Объединенных Наций неоднократно призывала к созданию постоянного механизма Организации Объединенных Наций по проблемам киберугроз в контексте международной безопасности. Приняв в октябре 2023 года решение Генеральной Ассамблеи о разработке программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, мы выполнили вышеупомянутый призыв.

В обсуждении будущего механизма был достигнут значительный прогресс, и Дания хотела бы высказать нижеследующие дополнительные соображения относительно будущего регулярного институционального диалога.

Такой институциональный диалог должен быть направлен на поддержку внедрения нормативных рамок, как это также было четко указано Рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2019–2021 года, которая пришла к выводу о том, что будущий институциональный диалог должен быть «практико-ориентированным процессом с конкретными целями, который основан на достигнутых ранее результатах и носить инклюзивный, прозрачный, консенсусный и нацеленный на результаты характер»¹.

Программа действий должна предусматривать постоянный институциональный механизм для контроля за выполнением согласованных норм, поддержки и содействия наращиванию потенциала, а также для предоставления и регулярного обновления рекомендаций. В то же время программа действий должна быть гибкой и должна позволять продолжать работу по совершенствованию нормативных рамок на основе опыта, накопленного в ходе выполнения действующих обязательств.

Дания считает крайне важным признать, что все заинтересованные стороны призваны играть значимую роль в формировании будущего кибербезопасности. Для обеспечения инклюзивного диалога необходимо предоставить соответствующим заинтересованным сторонам, в частности предприятиям, неправительственным организациям и научным кругам, возможность официально участвовать в консультациях и постоянно делиться своими соображениями. Это будет свидетельствовать о стремлении объединить различные точки зрения в рамках коллективного разума. Такое участие крайне важно для создания эффективного и всеобъемлющего диалога, направленного на решение многогранных проблем, которые касаются сферы кибербезопасности.

В рамках программы действий можно проводить ежегодные официальные заседания, а также технические совещания и заседания рабочих групп по соответствующим аспектам в течение всего года. В рамках будущего механизма следует созывать периодические обзорные конференции для обзора рамок ответ-

¹ [A/75/816](#), п. 74.

ственного поведения государств и, при необходимости, их обновления и определения стратегического направления работы механизма.

В оставшийся период работы текущей рабочей группы открытого состава необходимо посвятить время и усилия дальнейшей проработке аспектов программы действий. Чтобы обеспечить плавный переход к программе действий, необходимо обсудить, какие последствия для бюджета будет иметь создание постоянного механизма, и определить соответствующие структуры в Организации Объединенных Наций, которые будут выполнять эти функции в будущем.

Египет

[Подлинный текст на английском языке]
[26 февраля 2024 года]

I. Введение

1. Государства-члены разделяют растущую обеспокоенность международного сообщества по поводу расширения масштабов злонамеренного использования информационно-коммуникационных технологий (ИКТ) и чрезмерного развития рядом государств потенциала ИКТ в целях, несовместимых с международным правом и задачами поддержания международной стабильности и безопасности, что может негативно повлиять на защищенность инфраструктуры других государств в ущерб их безопасности как в гражданской, так и в военной областях.
2. Организация Объединенных Наций уже добилась прогресса в решении этих проблем благодаря оценкам и рекомендациям групп правительственных экспертов 2010, 2013, 2015 и 2021 годов, а также Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2021 года¹, создав тем самым кумулятивные и эволюционирующие рамки ответственного поведения государств при использовании ИКТ, разработанные с помощью этих процессов.
3. Государствам-членам рекомендуется при использовании ИКТ руководствоваться докладами групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы и докладом Рабочей группы открытого состава за 2021 год, а также первым и вторым ежегодными докладами о проделанной работе, представленными текущей рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Кроме того, в согласованных нормативных рамках подчеркивается, что международное право, и в частности Устав Организации Объединенных Наций, применимо и необходимо для поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды.
4. Существующая система норм, правил и принципов ответственного поведения государств при использовании ИКТ может снизить риски для международного мира, безопасности и стабильности, не ограничивая и не запрещая при этом действия, которые в остальном согласуются с нормами международного права.
5. Предлагаемая программа действий Организации Объединенных Наций по поощрению ответственного поведения государств при использовании ИКТ в контексте международной безопасности была инициирована в 2020 году Египтом и Францией и с тех пор дорабатывается межрегиональной группой государств, что отражено в заключительных докладах групп правительственных экспертов и в докладе Рабочей группы открытого состава за 2021 год, а также в первом и

¹ См. [A/65/201](#), [A/68/98](#), [A/70/174](#), [A/75/816](#) и [A/76/135](#).

втором ежегодных докладах о проделанной работе, представленных текущей рабочей группы открытого состава.

6. Генеральный секретарь опубликовал доклад (A/78/76), в котором обобщил мнения государств о сфере охвата, структуре, принципах, содержании, подготовительной работе и форматах учреждения программы действий.

7. Любой будущий механизм поддержания регулярного институционального диалога должен основываться на нормативной базе и существующих согласованных рамках, которые были одобрены Генеральной Ассамблеей на основе консенсуса.

8. Новый механизм или платформа должны быть созданы после завершения срока действия мандата действующей рабочей группы открытого состава после 2025 года. Это позволит избежать какого бы то ни было дублирования усилий или создания параллельных направлений работы. Такой механизм будет представлять собой универсальный центр и всеобъемлющую платформу под эгидой Организации Объединенных Наций для рассмотрения вопросов, связанных с достижениями в сфере информатизации и телекоммуникаций в контексте международной безопасности, и поощрения ответственного поведения государств при использовании информационно-коммуникационных технологий.

9. Государства-члены в принципе согласились с тем, что механизм поддержания регулярного институционального диалога будет возглавляться государствами и будет одновекторным, постоянным, инклюзивным, транспарентным и гибким².

II. Цели и сфера охвата будущего механизма Организации Объединенных Наций для поддержания регулярного институционального диалога

10. Служить платформой для регулярного институционального диалога, который позволит всем государствам-членам участвовать в одновекторном, постоянном, инклюзивном, прозрачном, ориентированном на практические действия, учитывающим достигнутые результаты и консенсусном процессе, который опирается на существующие нормативные рамки.

11. Содействовать созданию открытой, безопасной, стабильной, доступной, мирной и функционально совместимой среды ИКТ.

12. Предотвращать конфликты, возникающие в связи с использованием ИКТ, и обеспечивать урегулирование соответствующих споров мирными средствами.

13. Закрепить созданные киберсредства (реестр контактных пунктов и все другие предложения, которые будут приняты рабочей группой открытого состава) с целью поддержания их эффективного функционирования и пересмотра по мере необходимости.

14. Разработать конкретные рекомендации для оказания поддержки государствам-членам при внедрении ими согласованных норм, правил и принципов, в том числе путем содействия международному сотрудничеству и помощи.

15. Сфера его охвата должна быть ориентирована на следующие три компонента:

а) Реализация существующих согласованных итоговых документов.

Периодическая оценка хода внедрения согласованных нормативных рамок государствами-членами путем рассмотрения их соответствующих добровольных национальных докладов, которые должны составляться по согласованному унифицированному шаблону для представления отчетности;

² A/78/265, п. 55.

б) **Доработка существующих нормативных рамок.** Выявление пробелов и различных проблем, с которыми сталкиваются государства-члены при внедрении нормативных рамок, и поощрение выполнения соответствующих практических рекомендаций для решения этих проблем, а также возобновление обсуждения концептуальных вопросов, включая вопросы о применимости норм международного права и необходимости разработки новых нормативных положений и юридически обязывающих обязательств в этой области;

с) **Содействие наращиванию потенциала.** Принятие практических мер по развитию международного сотрудничества и периодическая оценка необходимости дополнительных действий для реагирования на текущие и возникающие проблемы с учетом быстро меняющейся среды; обмен информацией о передовом опыте, который может быть использован на национальном, региональном и международном уровнях (включая информацию о законодательной и административной базе и мерах по защите критически важной инфраструктуры); и оказание конкретной поддержки в наращивании потенциала на основе оценки государством-получателем собственных потребностей и в соответствии с принципами наращивания потенциала, содержащимися в документе [A/76/135](#). Следует предусмотреть специальный механизм финансирования соответствующих мероприятий, включая возможность использования как существующих, так и новых инструментов, таких как Многосторонний донорский целевой фонд Всемирного банка по кибербезопасности.

III. Создание будущего механизма поддержания регулярного институционального диалога

16. Мнения и материалы, представленные государствами-членами в рамках действующей рабочей группы открытого состава по предложению о программе действий и докладам Генерального секретаря в соответствии с резолюциями [77/380](#) и [78/237](#) Генеральной Ассамблеи, а также соответствующие потенциальные рекомендации, содержащиеся в докладах рабочей группы открытого состава, являются основой для учреждения такого механизма с точки зрения его сферы охвата, структуры и форматов.

17. Государствам-членам следует продолжать активно участвовать в работе действующей рабочей группы открытого состава, созданной в соответствии с резолюцией [75/240](#) Генеральной Ассамблеи, с целью подготовки консенсусных докладов, включая рекомендации по созданию будущего механизма поддержания регулярного институционального диалога.

18. Механизм следует доработать и усовершенствовать в рамках действующей рабочей группы открытого состава таким образом, чтобы избежать дублирования каких бы то ни было усилий или создания параллельных процессов и сохранить дух консенсуса при рассмотрении аспектов международной безопасности в сфере ИКТ по линии Организации Объединенных Наций.

19. Механизм будет создан после завершения срока действия мандата текущей рабочей группы открытого состава в 2025 году на основе рекомендаций заключительного доклада текущей рабочей группы открытого состава, при этом можно рассмотреть возможность налаживания будущего регулярного институционального диалога путем принятия консенсусной резолюции Генеральной Ассамблеи на основе всесторонних и прозрачных консультаций и подготовки. Государства-члены, возможно, договорятся в рамках действующей рабочей группы открытого состава о создании механизма на основе политической декларации, которая может быть одобрена в резолюции Генеральной Ассамблеи, в том числе о предлагаемом формате работы механизма. Итоговый документ Саммита будущего, возможно, будет содержать ссылку на первоначальное соглашение по этому вопросу.

IV. Структура и возможные форматы

Периодические совещания

20. Механизм, который может принять форму программы действий, должен предусматривать созыв каждые шесть лет обзорной конференции, которая будет посвящена следующим вопросам:

а) рассмотрение и обзор внедрения механизма, определение основных приоритетных направлений работы в последующие годы и в конечном счете принятие программы работы последующих совещаний;

б) изучение вопроса о необходимости разработки на основе консенсуса дополнительных норм, правил, принципов или обязательных к исполнению обязательств для обновления нормативных рамок.

21. Механизм должен предусматривать созыв регулярных двухгодичных совещаний для выполнения программы работы, которая будет приниматься обзорной конференцией, и анализа применения государствами-членами согласованных норм, правил и принципов на основе рассмотрения их периодических национальных докладов об имплементации.

22. Председатель каждой сессии созывает подготовительные консультативные совещания перед каждой обзорной конференцией и последующими двухгодичными совещаниями.

23. В рамках согласованного механизма на основе консенсуса может быть принято решение о проведении межсессионных совещаний или создании неофициальных рабочих групп для изучения конкретных смежных вопросов, включая применимость международного права и разработку новых норм, правил и принципов, а также юридически обязательных к исполнению обязательств или документов в зависимости от обстоятельств.

Доклады

24. В рамках согласованного механизма государствам-членам будет предложено добровольно представлять свои национальные доклады об имплементации каждые два года на ротационной основе, при этом минимум один доклад будет представляться раз в три цикла (каждые шесть лет). Этот процесс может опираться на типовой обзор хода реализации на национальном уровне рекомендаций Организации Объединенных Наций по ответственному использованию государствами ИКТ в контексте международной безопасности. Государствам-членам рекомендуется также включать в свои национальные доклады об имплементации раздел, в котором будут подробно изложены их приоритеты и потребности в области наращивания потенциала.

25. На каждом созываемом раз в два года совещании и обзорной конференции на основе консенсуса будет приниматься заключительный доклад, включая итоговый документ, который будет представляться на рассмотрение и одобрение следующей сессии Первого комитета.

Принятие решений

26. Принятие в рамках программы действий решений по вопросам существа осуществляется на основе консенсуса.

Секретариат

27. Обеспечивать секретариатское обслуживание механизма следует Управлению по вопросам разоружения.

Участие заинтересованных сторон

28. Механизм является межправительственным процессом, при котором ведение переговоров и принятие решений являются исключительной прерогативой государств-членов.
29. Механизм будет ориентирован на взаимодействие с соответствующими заинтересованными сторонами на систематической, устойчивой и конструктивной основе.
30. Соответствующие неправительственные организации, имеющие консультативный статус при Экономическом и Социальном Совете согласно его резолюции [1996/31](#), должны уведомлять секретариат о своем желании принять участие в работе механизма.
31. Другие заинтересованные неправительственные организации, имеющие отношение к сфере деятельности и целям механизма и обладающие компетентностью в этой области, должны также сообщать секретариату о своей заинтересованности в участии, представив информацию о своих целях, программах и деятельности в областях, имеющих отношение к сфере деятельности механизма. Соответственно, этим организациям будет предложено принять участие в официальных сессиях в рамках механизма в качестве наблюдателей на основе процедуры отсутствия возражений.
32. Аккредитованные заинтересованные стороны смогут присутствовать на официальных заседаниях в рамках программы действий, выступать с устными заявлениями на специальной сессии для заинтересованных сторон и представлять письменные материалы. Государствам-членам рекомендуется проявлять осмотрительность при использовании механизма отсутствия возражений с учетом принципа инклюзивности.
33. В тех случаях, когда высказываются возражения против включения в список той или иной неправительственной организации, возражающее государство-член доводит это до сведения Председателя механизма и на добровольной основе информирует Председателя об общих основаниях для своих возражений. По просьбе любого государства-члена Председатель знакомит его со всей полученной в этой связи информацией.
34. Председатель организует неофициальные консультативные совещания с заинтересованными сторонами в межсессионный период.
35. Механизм может способствовать координации усилий с соответствующими региональными и субрегиональными инициативами, в том числе в форме обеспечения их возможного участия и вклада в работу.

Эстония

[Подлинный текст на английском языке]
[30 апреля 2024 года]

В соответствии с резолюцией [78/237](#) Генеральной Ассамблеи, Эстония хотела бы представить национальную позицию по будущему регулярному институциональному диалогу по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ.

В последние годы угрозы, связанные с использованием ИКТ в контексте международной безопасности, продолжали усиливаться и претерпевать существенные изменения в нынешней сложной геополитической обстановке. Усиление угроз в сфере использования ИКТ приводит к росту проблем, связанных с

негативным влиянием на экономическое и социальное развитие, и сказывается на национальной и международной стабильности. Эти последствия остаются в центре внимания многосторонних дискуссий, о чем свидетельствует деятельность Группы правительственных экспертов и рабочей группы открытого состава.

После широкой поддержки межрегиональной группой стран предложения о разработке программы действий мы поддерживаем программу действий в качестве постоянного институционального механизма в рамках Первого комитета с акцентом на реализацию согласованных рамок ответственного поведения государств в киберпространстве, а также, при необходимости, на дальнейшее развитие этих рамок. Мы считаем, что такой регулярный институциональный диалог будет способствовать снижению напряженности, предотвращению конфликтов и использованию ИКТ в мирных целях.

Данная позиция страны представляет собой обновленный вариант национального вклада Эстонии, включенного в доклад Генерального секретаря о программе действий (A/78/76), который основывается, в частности, на прогрессе, отраженном в резолюции 78/16 Генеральной Ассамблеи, и обсуждениях в рамках рабочей группы открытого состава 2021–2025.

1. Программа действий должна основываться на существующей нормативной базе и нормативных рамках ответственного поведения государств с акцентом на использование государствами ИКТ в контексте международного мира и безопасности. Эстония считает, что ИКТ должны использоваться в соответствии с целями поддержания международной стабильности и безопасности и в соответствии с согласованной нормативной базой и рамками ответственного поведения государств. Мы подчеркиваем, что государствам-членам следует при использовании ИКТ руководствоваться докладами групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы и докладом Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2021 год. Механизм программы действий должен формироваться исходя из этих предпосылок и преследовать цель обеспечения открытой, стабильной, безопасной, доступной и мирной информационно-коммуникационной среды. Эстония считает, что некоторые существующие или предлагаемые инициативы, такие как создание глобального реестра контактных пунктов, могли бы обеспечить реальную поддержку в эффективном функционировании программы действий в таком формате.

2. Программа действий должна иметь нейтральный формат, обеспечивающий институциональную стабильность. С точки зрения малого государства необходимо иметь ясность и институциональную стабильность в отношении дальнейших процессов, связанных с обсуждением использования государствами ИКТ. Поэтому Эстония выступает за создание единой постоянной структуры для содействия дальнейшему обсуждению вопросов, которые рассматривались рабочей группой открытого состава, после завершения работы нынешней рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Мы поддерживаем дальнейшее обсуждение структуры, формата и сроков учреждения программы действий как механизма поощрения ответственного поведения государств при использовании ИКТ с учетом мнений всех государств-членов. Эстония поддерживает вариант создания механизма на основе международной конференции, как это было согласовано в резолюции 77/37 Генеральной Ассамблеи, не позднее 2026 года. Эстония считает, что предлагаемый формат программы действий избавит Ассамблею от необходимости обсуждать вопрос о создании новых киберпроцессов каждые два, три или четыре года. Мы надеемся, что нормативные рамки программы действий

будут восприниматься государствами-членами как полезная и нейтральная система и что не будет необходимости в параллельных процессах.

3. Программа действий должна стать целостной основой для рассмотрения различных тем, предложенных рабочей группой открытого состава, при широком участии. Мы приветствуем растущий интерес государств-членов к участию в обсуждении различных тем, которые рассматриваются в ходе текущих дебатов на заседаниях рабочей группы открытого состава. Текущие обсуждения в рамках рабочей группы открытого состава были весьма содержательными, и различные государства-члены предложили целый ряд идей. Мы считаем, что механизм программы действий может стать для государств-членов «удобной» площадкой для постановки вопросов, связанных с ИКТ и международным миром и безопасностью. Поэтому программа действий может стать целостной основой для выдвижения и более детального анализа этих идей.

4. Программа действий должна также предусматривать четкие и прозрачные форматы для конструктивного участия сообщества многих заинтересованных сторон с целью дальнейшего использования их опыта и знаний. Взаимодействие с сообществом многих заинтересованных сторон поможет государствам-членам внедрить нормативные рамки ответственного поведения государств и разработать и принять обусловленные потребностями меры по наращиванию потенциала для укрепления глобального потенциала противодействия киберугрозам. Кроме того, программа действий могла бы также активизировать региональное взаимодействие за счет сотрудничества с региональными и профильными организациями, чтобы использовать и развивать текущие смежные инициативы.

5. Программа действий должна обеспечить более гибкий, но в то же время сфокусированный формат для продолжения дискуссий о нормативных рамках ответственного поведения государств. Эстония хотела бы подчеркнуть, что при разработке нормативных рамок программы действий следует также учитывать проблемы, связанные с ограниченными возможностями малых государств, и, следовательно, исходить из разумных ожиданий в отношении прогнозируемого объема работы:

а) мы предлагаем включить в качестве элементов механизма программы действий ежегодные пленарные заседания, на которых будут рассматриваться темы, относящиеся к основным компонентам нормативных рамок ответственного поведения государств;

б) мы также поддерживаем идею проведения предметных дискуссий в формате рабочих групп, открытых для участия всех заинтересованных сторон, в том числе по вопросам, касающимся угроз, наращивания потенциала, укрепления доверия, норм и международного права. Другим вариантом может быть более целенаправленное рассмотрение в этих рабочих группах узкотематических вопросов, таких как защита объектов критически важной инфраструктуры. Участие в рабочих группах должно быть добровольным, а решение о создании таких рабочих секций будет приниматься государствами на ежегодных пленарных заседаниях;

в) мы также поддерживаем идею проведения обзорных конференций (например, раз в четыре года), которые позволят участникам оценить достигнутый прогресс и рассмотреть дальнейшие возможные поправки к мандату, а также к организации работы или программе действий.

6. Среди прочих тем программа действий должна предусматривать механизм широкого участия в обсуждениях по проблематике международного права. Эстония приветствует все более активные и содержательные обсуждения

международного права и того, как оно применимо к сфере использования государствами ИКТ. Государства-члены выиграют от более глубокого понимания и единства мнений относительно применения действующих норм, а также от более детального анализа любых возможных пробелов. Программа действий будет иметь все шансы стать общедоступной площадкой для продолжения этих обсуждений. В частности, программа действий может стать платформой для обсуждения следующих элементов международного права: а) дальнейшее обсуждение вопроса о том, как международное право применимо к киберпространству; б) обмен национальными мнениями; в) проведение специальных заседаний, посвященных вопросу о том, как международное право применяется к использованию ИКТ, с акцентом на конкретные темы для более детального обсуждения; д) брифинги экспертов; е) обсуждения сценарных анализов; и ф) наращивание потенциала в области международного права.

7. Программа действий должна быть ориентирована на практические действия с особым акцентом на наращивание потенциала. Неотъемлемой частью дальнейших дискуссий должен стать вопрос о внедрении согласованных нормативных рамок ответственного поведения государств. Кроме того, в рамках программы действий можно предусмотреть добровольную отчетность о национальных усилиях по имплементации, что будет способствовать достижению многих целей, таких как укрепление доверия, обеспечение транспарентности, а также картирование потенциала и потребностей. Программа действий должна учитывать существующие инициативы по наращиванию потенциала на хорошо скоординированной и взаимодополняемой основе. В частности, при разработке программы действий следует учитывать существующие мероприятия и ресурсы по оценке потребностей, такие как портал “Cybil” и портал Европейского союза “CyberNet”, которые позволяют вести учет проектов по созданию киберпотенциала в государствах — членах Европейского союза.

Франция

[Подлинный текст на французском языке]
[30 апреля 2024 года]

I. Введение

Уже более 20 лет правительства признают, что цифровые технологии являются катализатором прогресса и развития человечества, но что при этом они могут использоваться в целях, несовместимых с задачей поддержания международной стабильности и безопасности.

С 2003 года Первый комитет Генеральной Ассамблеи создал ряд рабочих групп, которые занимаются вопросами поддержания международного мира, безопасности и стабильности в цифровой среде. С этой целью они составили рамочные принципы ответственного поведения государств при использовании цифровых технологий, которые Генеральная Ассамблея одобрила консенсусом в ряде резолюций¹.

Рабочие группы также обсуждали вопрос о поддержании регулярного институционального диалога для рассмотрения проблем, связанных с использованием цифровых технологий в контексте международной безопасности.

Было подчеркнуто, что такой диалог должен быть направлен, в частности, на поддержку реализации вышеуказанных рамочных принципов. В частности,

¹ См. резолюции [70/237](#) и [76/19](#) Генеральной Ассамблеи.

Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2019–2021 пришла к выводу о том, что будущий регулярный институциональный диалог «должен быть практико-ориентированным процессом с конкретными целями, опирающимся на достигнутые ранее результаты и носящим инклюзивный, прозрачный, консенсусный и нацеленный на результаты характер»². Государства также особо отметили «пользу изучения механизмов, предназначенных для контроля за осуществлением согласованных норм и правил»³.

Кроме того, государства отметили, что вышеуказанные рамочные принципы носят кумулятивный и эволюционирующий характер и что со временем могут быть разработаны дополнительные нормы. Они также отмечали возможность разработки в будущем, при необходимости, дополнительных обязательств, имеющих обязательную силу⁴. Будущий регулярный институциональный диалог должен способствовать реализации согласованных рамочных принципов, но также допускать возможность их доработки в будущем, особенно ввиду возникновения новых вызовов и угроз.

В этом контексте предложение по учреждению программы действий, представленное в 2020 году межрегиональной группой государств, обеспечит Первому комитету постоянный институциональный механизм мониторинга осуществления рамочных принципов и при необходимости дальнейшей их разработки.

В своем докладе о программе действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности (A/78/76) Генеральный секретарь рекомендовал государствам продолжать обсуждать потенциальную сферу охвата, структуру, принципы, содержание, функции и механизм контроля за осуществлением предлагаемой программы действий под эгидой рабочей группы открытого состава (2021–2025 годы) с учетом мнений, изложенных в докладе, а также результатов региональных и субрегиональных консультаций, организованных Управлением по вопросам разоружения в соответствии с резолюцией 77/37 Генеральной Ассамблеи.

Настоящее представление является обновленным вариантом представленного Францией материала, включенного в документ A/78/76, и отражает прогресс, достигнутый благодаря резолюции 78/16 Генеральной Ассамблеи и продолжающимся обсуждениям в рамках Рабочей группы открытого состава 2021–2025.

II. Сфера охвата и цели

В качестве механизма Первого комитета программа действий будет предусматривать рассмотрение вопросов, связанных с использованием цифровых технологий в контексте международной безопасности. Ее основной целью будет внесение вклада в поддержание международного мира и безопасности путем обеспечения открытой, безопасной, стабильной, доступной и мирной цифровой среды.

С этой целью задачами программы действий должны быть:

- сотрудничество: для снижения напряженности, предотвращения конфликтов и содействия использованию цифровых технологий в мирных целях на

² A/75/816, приложение I, п. 74.

³ A/75/816, приложение I, п. 73.

⁴ Резолюция 76/19 Генеральной Ассамблеи, десятый пункт преамбулы.

основе совместного подхода к противодействию киберугрозам и инклюзивного диалога между государствами и с заинтересованными сторонами;

- стабильность: для содействия стабильности в киберпространстве за счет поддержки осуществления и при необходимости дальнейшей разработки рамок ответственного поведения государств на основе международного права, включая международное гуманитарное право и право прав человека, нормы ответственного поведения государств, меры укрепления доверия и меры по наращиванию потенциала;
- устойчивость: для внесения вклада в преодоление цифрового разрыва и повышения глобальной жизнестойкости путем осуществления рамок ответственного поведения государств.

III. Структура и содержание

Организационная структура

Программа действий могла бы основываться на директивном документе, который будет, в частности, иметь целью:

а) подтвердить политическую приверженность государств рамочным принципам ответственного поведения государств, закрепленным в соответствующих резолюциях и докладах⁵. Эта приверженность будет базироваться на консенсусных итоговых документах, одобренных Рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, касающихся, в частности, создания глобального межправительственного реестра контактных пунктов, возможного создания глобального портала по сотрудничеству, а также идеи о составлении реестра угроз. Будущая программа действий должна базироваться на этих консенсусных итоговых документах⁶;

б) создать постоянный институциональный механизм с целью: i) содействовать осуществлению рамочных принципов, в том числе с помощью соответствующих мер по наращиванию потенциала государств; ii) дальнейшего совершенствования рамочных принципов по мере необходимости; iii) поощрения сотрудничества между широким кругом заинтересованных сторон в соответствующих областях.

Программа действий в качестве постоянного механизма могла бы иметь следующую организационную структуру:

- регулярные пленарные совещания, которые можно было бы проводить на ежегодной основе или раз в два года (Франция открыта для дальнейшего обсуждения оптимальной периодичности таких совещаний с учетом возможностей государств и необходимости идти в ногу с последними достижениями в цифровой сфере). Эти совещания позволят: а) обсуждать существующие и возникающие угрозы; б) рассматривать ход внедрения на практике норм, правил и принципов; в) продолжать обсуждения по вопросу о том, каким образом международное право применяется к использованию

⁵ В частности, в резолюции 76/19 Генеральной Ассамблеи, консенсусных докладах групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы, докладе Рабочей группы открытого состава 2019–2021 за 2021 год и первом ежегодном докладе о деятельности рабочей группы открытого состава 2021–2025 с учетом того, что будущие консенсусные итоговые документы нынешней рабочей группы дополняют эти рамочные принципы, которые носят кумулятивный и эволюционирующий характер.

⁶ См. резолюцию 77/37 Генеральной Ассамблеи, второй пункт преамбулы, и резолюцию 78/16 Генеральной Ассамблеи, второй пункт преамбулы.

цифровых технологий и выявлять потенциальные пробелы; d) обсуждать применение мер укрепления доверия; e) определять приоритеты в области наращивания потенциала, в том числе на основе добровольного представления отчетности; f) намечать меры, которые следует принять в будущем, и составлять программу работы межсессионных заседаний. На ежегодных совещаниях могут приниматься консенсусные решения о создании технических рабочих секций, которые будут открыты для участия всех государств и заинтересованных сторон и будут рассматривать конкретные вопросы (см. ниже). Следует поощрять участие технических экспертов и юристов;

- межсессионные заседания, которые будут способствовать выполнению программы работы, согласованной на ежегодных совещаниях. Эти заседания могут принимать форму технических совещаний или рабочих групп открытого состава по конкретным рабочим секциям в соответствии с приоритетами и рабочими областями, определенными на ежегодных совещаниях;
- обзорные конференции, которые могут проводиться, например, раз в четыре года для рассмотрения необходимости обновления и — если это целесообразно — дальнейшего совершенствования рамочных принципов (см. ниже). Можно было бы создать специальную рабочую секцию для проведения более обстоятельных обсуждений по вопросу о том, каким образом международное право применяется к использованию цифровых технологий, и для выявления пробелов в рамочных принципах, которые могли бы обусловить необходимость дальнейшего их совершенствования.

Содержание

а) Содействие практической реализации рамочных принципов

В рамках программы действий будет поощряться добровольное представление отчетности о принятых национальных мерах по практической реализации рамочных принципов либо с помощью создания специальной системы отчетности, либо с помощью поощрения использования существующих механизмов (таких как типовой национальный обзор выполнения рекомендаций Института Организации Объединенных Наций по исследованию проблем разоружения или национальные доклады Генеральному секретарю). Такого рода отчетность позволит определить приоритеты в отношении практической реализации рамочных принципов и оценить потребности в наращивании потенциала.

На ежегодных совещаниях по программе действий можно принимать и регулярно обновлять практические рекомендации относительно национальных усилий по практической реализации рамочных принципов. В рамках вышеуказанной организационной структуры на ежегодных совещаниях по программе действий можно было бы создать технические совещания или рабочие группы открытого состава для продолжения обсуждений по конкретным вопросам, связанным с практической реализацией рамочных принципов.

Например, на ежегодном совещании можно определить приоритетную тему применительно к практической реализации рамочных принципов (применение конкретной нормы или меры укрепления доверия, безопасность цифровых продуктов и услуг, защита критической инфраструктуры и т. д.). Чтобы содействовать обмену мнениями по этой теме, привлечению технических экспертов и обсуждению соответствующей передовой практики и возникающих трудностей, на ежегодном совещании можно создать специальную рабочую секцию,

участие в которой будет открыто для всех государств и деятельность которой будет осуществляться на межсессионных заседаниях по программе действий.

Выводы и рекомендации по итогам работы этих технических совещаний или рабочих групп открытого состава будут представляться на следующем пленарном заседании.

Программа действий будет обеспечивать поддержку мер по наращиванию потенциала в области практической реализации рамочных принципов и будет направлена на активизацию многостороннего сотрудничества в этой области, а также координацию усилий с другими соответствующими инициативами.

- Государствам предлагается рассмотреть вопрос о создании в рамках будущей программы действий добровольного фонда для финансирования некоторых видов деятельности, направленной на поощрение внедрения рамок ответственного поведения государств. Прообразом такого фонда может быть Целевой фонд Организации Объединенных Наций в поддержку сотрудничества в сфере регулирования вооружений⁷. Инициативы или проекты, финансируемые этим фондом, должны соответствовать кругу полномочий, который можно определить на первом совещании программы действий (поощрение соблюдения рамочных принципов, соблюдение руководящих принципов наращивания потенциала, согласованных в заключительном докладе Рабочей группы открытого состава 2019–2021 и т. д.).
- Программа действий будет также использоваться для оптимизации существующих усилий и инициатив. Совещания по программе действий и межсессионные заседания технической рабочей группы по наращиванию потенциала позволят государствам обсуждать приоритеты в области наращивания потенциала (с учетом потребностей, определенных благодаря добровольному представлению отчетности), а заинтересованным сторонам представлять соответствующие инициативы. В рамках программы действий можно было бы разработать систему «сертификации» в целях поддержки и поощрения деятельности, соответствующей ее целям.
- Представители других организаций (таких как Международный союз электросвязи или Многосторонний донорский целевой фонд Всемирного банка по кибербезопасности) могли бы проводить брифинги на совещаниях по программе действий в целях обеспечения координации и взаимодополняемости мер по наращиванию потенциала, принимаемых различными структурами (в пределах мандата и сферы компетенции каждой из структур).

в) Совершенствование рамочных принципов

Чтобы находить ответы на новые вызовы, рамочные принципы можно обновлять по мере необходимости на регулярных совещаниях или обзорных конференциях на основе консенсуса (обеспечивая возможность проведения обсуждений о дальнейшем развитии рамок, в том числе путем углубления общего понимания норм и того, как существующие положения международного права применяются при использовании цифровых технологий, выявления пробелов в этом понимании и, где это целесообразно, рассмотрения вопроса о необходимости в дополнительных добровольных, не имеющих обязательной силы нормах или дополнительных имеющих обязательную юридическую силу обязательствах)⁸.

⁷ Целевой фонд Организации Объединенных Наций в поддержку сотрудничества в сфере регулирования вооружений, см. <https://disarmament.unoda.org/unscar/>.

⁸ См. резолюцию 78/16 Генеральной Ассамблеи, пункт 3 b).

с) Участие широкого круга заинтересованных сторон

Памятуя о том, что «государства несут главную ответственность за поддержание международного мира и безопасности»⁹ и что они должны по-прежнему играть центральную роль (в том числе обладать исключительными полномочиями на принятие решений) в любом процессе в Первом комитете, Франция поддерживает расширение диалога и сотрудничества с заинтересованными сторонами в контексте будущей программы действий.

- Принятие решений и согласование итоговых документов остается исключительной прерогативой государств.
- Вместе с тем ценность дальнейшей активизации при необходимости сотрудничества с гражданским обществом, частным сектором, научно-образовательными кругами и техническим сообществом неоднократно подчеркивалась соответствующими рабочими группами Первого комитета¹⁰. Сотрудничество с этими субъектами может быть критическим для выполнения государствами своих обязательств согласно рамкам ответственного поведения. Кроме того, эти заинтересованные стороны сами «обязаны использовать ИКТ [информационно-коммуникационные технологии] таким образом, чтобы не создавать угрозу миру и безопасности»¹¹. Частные субъекты могут также привнести в дискуссии свой ценный опыт и оказать содействие в осуществлении усилий по наращиванию потенциала.
- Поэтому организационные процедуры проведения совещаний по программе действий должны позволять заинтересованным сторонам участвовать в официальных сессиях, выступать с заявлениями и представлять свои материалы, как в случае других процессов в Первом комитете, где их опыт играет полезную роль, таким как Группа правительственных экспертов по новым технологиям в области смертоносных автономных систем вооружений, созываемая в рамках Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие¹². Такие процедуры будут способствовать повышению транспарентности процесса, позволяя проводить диалог с участием многих заинтересованных сторон в официальной обстановке.
- Чтобы обеспечить широкое представительство на этих совещаниях, следует поощрять и поддерживать участие заинтересованных сторон от каждой региональной группы, в том числе с помощью специальных спонсорских программ.

⁹ A/75/816, приложение I, п. 10.

¹⁰ A/75/816, приложение I, п. 22.

¹¹ A/75/816, приложение I, п. 10.

¹² См. правило 49 правил процедуры Конвенции о запрещении или ограничении применения конкретных видов обычного оружия, которые могут считаться наносящими чрезмерные повреждения или имеющими неизбирательное действие (принятой в 2016 году в рамках пятой Конференции Высоких Договаривающихся Сторон Конвенции по рассмотрению действия Конвенции).

IV. Формы учреждения и работа по подготовке к учреждению программы действий

Подготовительная работа

Франция поддерживает продолжение целенаправленных и специальных дискуссий в Рабочей группе открытого состава 2021–2025 по дальнейшей разработке программы действий и достижению консенсуса о ее учреждении.

В своих заключительных докладах Рабочая группа открытого состава 2019–2021 и Группа правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности рекомендовали доработать программу действий, в том числе в рамках Рабочей группы открытого состава 2021–2025. Рабочая группа открытого состава 2021–2025 также призвала провести целенаправленные дискуссии по программе действий в своем докладе о ходе работы за 2022 год.

Региональные консультации, проведенные в 2023 году, и доклад Генерального секретаря (A/78/76) позволили собрать мнения большой и разнообразной группы государств. В докладе Генерального секретаря подчеркивается целесообразность рассмотрения предложения о программе действий при широком участии и в атмосфере открытости с твердой опорой на ранее достигнутые консенсусные договоренности и прогресс в работе, проделанной в Генеральной Ассамблее. В рамках своего второго ежегодного доклада о своей деятельности Рабочая группа открытого состава 2021–2025 приложила усилия в этом направлении, согласовав в принципе «общие элементы»¹³, по которым можно достичь консенсуса, чтобы конструктивным образом выработать общую концепцию будущего механизма регулярного институционального диалога.

В своей резолюции 77/37 Генеральная Ассамблея просила Генерального секретаря представить ей доклад по программе действий, который будет служить основой для дальнейших дискуссий в Рабочей группе открытого состава 2021–2025. В своей резолюции 78/16 Генеральная Ассамблея подчеркнула, что Рабочая группа открытого состава 2021–2025 должна играть центральную роль в дальнейшей работе над программой действий в целях учреждения этой программы по завершении деятельности рабочей группы и не позднее 2026 года.

Таким образом, межсессионные заседания и специальные сессии Рабочей группы открытого состава 2021–2025 следует провести в 2024 и 2025 годах для дальнейшей проработки различных аспектов программы действий и составления проекта ее учредительного документа.

Учреждение

Франция выступает за продолжение дискуссий по конкретным формам потенциального учреждения программы действий, в том числе на специальной конференции.

В своей резолюции 77/37 Генеральная Ассамблея ссылалась на созыв «международной конференции» как на вариант учреждения программы действий (как это было сделано в случае Программы действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней). В своей резолюции 78/16 Генеральная Ассамблея постановила учредить по завершении работы Рабочей группы открытого состава 2021–2025 и не позднее 2026 года механизм под эгидой Организации Объединенных Наций, который будет постоянным, инклюзивным и

¹³ A/78/265, п. 55.

ориентированным на практические действия и который будет иметь конкретные цели, как это указано в резолюции 77/37, и общие элементы для будущего регулярного институционального диалога, согласованные консенсусом во втором докладе рабочей группы открытого состава 2021–2025 о проделанной работе за год. Если государства примут такое решение, такую конференцию можно созвать в 2025 году для принятия учредительного документа вышеуказанного механизма на основе подготовительной работы, проделанной Рабочей группой открытого состава 2021–2025.

Эта международная конференция должна принимать решения на основе консенсуса, по крайней мере по вопросам существа. Соответствующие заинтересованные стороны должны быть допущены к участию (они могут быть аккредитованы таким же образом, как и участники сессий Специального комитета по разработке всеобъемлющей международной конвенции по борьбе с использованием информационно-коммуникационных технологий в преступных целях, как это предусмотрено в резолюции 75/282 Генеральной Ассамблеи).

Генеральная Ассамблея затем может принять резолюцию, приветствующую итоги конференции, и постановить созвать первое заседание нового механизма.

Грузия

[Подлинный текст на английском языке]
[20 марта 2024 года]

Что касается будущего регулярного институционального диалога по вопросу об использовании информационно-коммуникационных технологий под эгидой Организации Объединенных Наций, то Грузия рассматривает программу действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности как оптимальный подход к продвижению инициатив Организации Объединенных Наций в области обеспечения кибербезопасности и ответственного поведения государств в киберпространстве.

В условиях текущей обстановки в плане безопасности, характеризующейся непредсказуемым и стремительным развитием геополитических событий, некоторые субъекты угрожают международному порядку, основанному на правилах, применяя сочетание традиционных и нетрадиционных методов ведения войны. К сожалению, бывают случаи, когда некоторые субъекты нарушают международное право в ходе киберопераций.

Мировое сообщество должно настойчиво привлекать таких субъектов к ответственности за их незаконное и неприемлемое поведение в киберпространстве, обеспечивая правовые последствия таких действий.

Программа действий может стать подходящей платформой для целенаправленных диалогов по вопросам применения международного права в киберпространстве после завершения в 2025 году работы нынешней рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025.

Мы выступаем за то, чтобы программа действий стала для Первого комитета единой платформой, посвященной решению проблем в сфере кибербезопасности, и послужила надежной структурой, позволяющей реализовывать инициативы, ориентированные на конкретные действия, и добиваться ощутимых результатов.

Отсутствие возможностей в национальном, региональном и глобальном масштабах представляет собой серьезную проблему. Поэтому программа действий должна способствовать национальным усилиям по введению в действие нормативных рамок и предусматривать оказание помощи в наращивании потенциала для сокращения цифрового разрыва.

Грузия приветствует создание глобального межправительственного реестра контактных пунктов. Эта инициатива знаменует собой значительный шаг вперед в укреплении международного сотрудничества и координации в области обеспечения кибербезопасности в контексте Организации Объединенных Наций.

Ввиду стремительных темпов развития информационно-коммуникационных технологий будущие международные рамки должны быть достаточно гибкими, чтобы в дальнейшем сохранять свою актуальность. Такой международный форум должен предусматривать механизм, который позволит периодически пересматривать соответствующие рамки на основе консенсуса в ходе регулярных пленарных заседаний или обзорных конференций. На этих заседаниях можно пересматривать действующие рамки и, если это целесообразно, принимать решения об их дальнейшем совершенствовании или доработке.

Грузия решительно поддерживает прозрачный и инклюзивный подход с участием многих заинтересованных сторон, подчеркивая активное участие как государственных, так и негосударственных субъектов в рамках институционального диалога по этим вопросам.

Германия

[Подлинный текст на английском языке]
[30 апреля 2024 года]

А. Основополагающие принципы программы действий

Германия поддерживает учреждение программы действий в качестве ориентированного на практические действия, постоянного, транспарентного, гибкого и инклюзивного форума для поддержания регулярного институционального диалога по вопросам безопасности в сфере использования ИКТ и самих ИКТ в рамках Первого комитета. Программа действий должна стать одновекторным механизмом последующей деятельности нынешней рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025. Он должен начать функционировать не позднее 2026 года для реализации результатов деятельности рабочей группы после завершения срока действия ее мандата в соответствии с решением, содержащимся в резолюции 78/16 Генеральной Ассамблеи, о создании механизма под эгидой Организации Объединенных Наций с конкретными целями, подтвержденными в резолюции 78/37, и с общими элементами, согласованными в принятом консенсусом втором ежегодном докладе рабочей группы открытого состава 2021–2025 о проделанной работе (A/78/265).

Необходимо избегать параллельных процессов и двойных структур, чтобы не перегружать возможности государств полноценно участвовать и обеспечивать проведение обсуждений, ориентированных на конкретные действия. Для подготовки к плавному переходу государствам необходимо продолжить обсуждение сферы охвата, структуры и содержания программы действий в рамках нынешней рабочей группы открытого состава с целью достижения консенсуса по существу и форматам осуществления программы действий. Цель должна заключаться в том, чтобы все государства-члены одобрили такую программу действий

на специальной конференции, которая будет проведена сразу же после последней сессии рабочей группы в 2025 году.

Общая цель программы действий заключается в содействии международному миру и безопасности в киберпространстве путем налаживания диалога и сотрудничества между государствами по вопросам имплементации существующих международных нормативных рамок ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ). Это потребует:

- наращивания киберпотенциала в соответствии с руководящими принципами, согласованными в заключительном докладе за 2021 год Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также согласованными принципами создания потенциала, подтвержденными в приложении С ко второму ежегодному докладу о проделанной работе. Использование возможностей взаимодействия с механизмами других форумов поможет избежать дублирования структур и растраты ресурсов;
- принятия мер укрепления доверия, включая эффективное осуществление первоначального, неисчерпывающего перечня мер укрепления доверия, согласованного во втором ежегодном докладе о проделанной работе (A/78/265, приложение В), в частности мер по созданию глобального реестра контактных пунктов;
- обмена передовым опытом на международном, межрегиональном и региональном уровнях;
- конструктивного участия соответствующих заинтересованных сторон.

Кроме того, программа действий должна стать постоянной платформой для содействия обсуждению существующих и возникающих угроз, а также вопроса о применимости международного права, включая международное гуманитарное право и права человека, в сфере использования ИКТ государствами. В рамках программы действий возможно дальнейшее обсуждение и, в соответствующих случаях, совершенствование международных нормативных рамок ответственного поведения государств в киберпространстве с целью их адаптации и реагирования на новые угрозы по мере их возникновения.

Программа действий должна обеспечить универсальную институциональную основу для других механизмов в области обеспечения кибербезопасности, которые в настоящее время готовятся в рамках рабочей группы, таких как киберпортал, по предложению Индии, и киберхранилище, по предложению Кении.

Главная цель, конкретные задачи и основополагающие принципы программы действий должны быть закреплены в форме политической декларации, которая должна быть согласована Генеральной Ассамблеей. Декларацию следует дополнить резолюцией Первого комитета с описанием задач, структуры и формата программы действий. Как политическая декларация, так и резолюция Первого комитета должны основываться на итоговом документе специальной конференции, которая должна состояться в 2025 году, как упоминалось выше.

В. Задачи, структура и формат программы действий

С учетом уроков, извлеченных из предыдущих и существующих документов, задачи программы действий должны быть сформулированы таким образом, чтобы обеспечить эффективное, широкое и прозрачное участие государств и позволить измерить прогресс в имплементации нормативных рамок ответственного поведения государств, в том числе с помощью механизма добровольной

ответственности, такого как национальный обзор выполнения рекомендаций Организации Объединенных Наций по ответственному использованию государствами ИКТ в контексте международной безопасности Института Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР). Нарращивание потенциала и сотрудничество как между государствами, так и с региональными организациями и негосударственными субъектами являются ключевыми факторами действий в тех областях, в которых процесс национальной имплементации идет медленно.

С учетом общих элементов, согласованных в принятом консенсусом втором ежегодном докладе о проделанной работе, структура и формат программы действий должны включать:

- a) проведение ежегодных конференций в Центральных учреждениях в Нью-Йорке в целях:
 - i) анализа и оценки прогресса в имплементации нормативных рамок и выполнении определенных задач;
 - ii) обсуждения возможного совершенствования нормативных рамок, в том числе путем углубления общего понимания применимости международного права в киберпространстве;
 - iii) принятия решений по конкретным темам;
 - iv) обмена информацией о существующих и возникающих угрозах международному миру и безопасности, связанных с использованием ИКТ;
 - v) дальнейшей разработки мер по наращиванию киберпотенциала;
 - vi) рассмотрения возможности дальнейшего поэтапного совершенствования программы действий с учетом потребностей государств-членов, принимая во внимание изменения в характере угроз и исходя из понимания того, что программа действий является гибким инструментом;
- b) осуществление и дальнейшую разработку мер по укреплению доверия с использованием глобального реестра контактных пунктов, который был создан нынешней рабочей группой открытого состава. Помимо того, что реестр сам по себе является мерой укрепления доверия, он должен служить основой для реализации глобального неисчерпывающего перечня мер укрепления доверия, согласованного во втором ежегодном докладе о проделанной работе, с общей целью снижения риска недопонимания и конфликтов в киберпространстве. Он также должен использоваться для обсуждения, принятия и осуществления дополнительных мер укрепления доверия на глобальном уровне. Способствуя разработке и осуществлению специальных мер по укреплению доверия, реестр станет центральным элементом программы действий, обеспечивающим концентрацию внимания на имплементации существующих нормативных рамок;
- c) проведение обзорных конференций каждые четыре — шесть лет, чтобы обеспечить возможность адаптации программы действий с учетом динамичной трансформации киберпространства и связанных с ним рисков для международного мира и безопасности;
- d) выполнение Управлением по вопросам разоружения функций секретариата программы действий. Помимо подготовки ежегодных совещаний и обзорных конференций, Управление также будет отвечать за ведение глобального реестра контактных пунктов и другие меры укрепления доверия;
- e) предоставление ЮНИДИР соответствующих инструментов мониторинга и обзора государствам (например, протоколов проверки применения норм,

согласно принятому консенсусом второму ежегодному докладу о проделанной работе) и проведение исследовательских мероприятий, связанных с имплементацией нормативных рамок;

f) возможность проведения дополнительных заседаний технических рабочих секций в межсессионный период. Специальные технические рабочие секции могут заниматься, среди прочего, такими темами, как наращивание киберпотенциала, меры укрепления доверия, применение международного права, включая международное гуманитарное право, а также текущие и возникающие угрозы. Участие в рабочих секциях должно быть добровольным, открытым для всех государств и регионально сбалансированным. Количество и формат рабочих секций, включая участие заинтересованных сторон, периодичность заседаний и возможности применения смешанных форматов работы, должны определяться с учетом возможностей полноценного участия государств и утверждаться на основе консенсуса на ежегодных совещаниях.

Государства будут обладать исключительным правом вести переговоры об итоговых документах и принимать решения в рамках программы действий. В то же время в программе следует предусмотреть механизмы взаимодействия с неправительственными заинтересованными сторонами (многосторонними и региональными организациями, гражданским обществом, частным сектором и научными кругами). Программа действий должна предусматривать возможности для широкого и конструктивного участия заинтересованных сторон, аналогичные условиям Специального комитета по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях (в частности, любое вето государства-члена на участие заинтересованной стороны должно быть публично обосновано; исключение заинтересованных сторон будет решаться путем голосования). Это включает право выступать и представлять письменные материалы на совещаниях, обзорных конференциях и дополнительных заседаниях технических рабочих секций в межсессионный период. Кроме того, для большинства форматов работы следует предусмотреть гибридные варианты участия, чтобы повысить инклюзивность обсуждений.

В первую очередь в области мер укрепления доверия и наращивания потенциала следует использовать существующие инициативы и структуры на региональном и субрегиональном уровнях или на других форумах и добиваться эффекта синергии (например, с региональными организациями, Многосторонним донорским целевым фондом Всемирного банка по кибербезопасности и Глобальным форумом по обмену опытом в области компьютерных технологий).

Существующие механизмы финансирования на других форумах Организации Объединенных Наций, такие как фонд «Структура по спасению жизней» или Целевой фонд Организации Объединенных Наций в поддержку сотрудничества в сфере регулирования вооружений в области контроля над вооружениями, могут стать ценными ориентирами при создании механизма поддержки усилий по наращиванию киберпотенциала в форме обучения и обмена передовым опытом. Кроме того, можно предусмотреть программу стипендий для содействия широкому представительству делегаций столиц развивающихся стран.

Можно создать добровольную межрегиональную «систему партнерства», в рамках которой государство, обладающее высоким потенциалом в области имплементации нормативных рамок ответственного поведения государств в киберпространстве, будет работать в паре с одним или несколькими государствами с более низким потенциалом. Такой механизм будет способствовать укреплению сотрудничества между государствами, налаживанию диалога и обмену передовым опытом, а также расширению возможностей государств по имплементации

норм в целом. В качестве эталонной модели в этом отношении можно использовать инициативу Организации по безопасности и сотрудничеству в Европе под названием «прими меру укрепления доверия».

Ирландия

[Подлинный текст на английском языке]

[1 мая 2024 года]

Поскольку Ирландия относится к числу стран с открытым обществом и сильно взаимосвязанной цифровой экономикой, она остро осознает проблему ухудшения международной обстановки в области безопасности, особенно в связи с ростом злонамеренной активности с использованием киберсредств. Осознавая эту проблему, мы принимаем меры на национальном уровне и совместно с нашими партнерами по Европейскому союзу, чтобы повысить степень устойчивости, укрепить наш потенциал по выявлению, предотвращению и сдерживанию угроз, а также способствовать созданию глобального, открытого и безопасного киберпространства, в основе которого лежат международное право и права человека.

При этом мы однозначно придерживаемся того мнения, что глобальный характер этой проблемы требует принятия всеобъемлющих международных мер реагирования. Ирландия поддерживает и с удовлетворением отмечает разработку на основе консенсуса нормативных рамок Организации Объединенных Наций по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ). Нормативные рамки стали важнейшим результатом множества принятых консенсусом рекомендаций групп правительственных экспертов (2010, 2013, 2015 и 2021 годов) и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (2021 года). В двух последних принятых консенсусом ежегодных докладах о проделанной работе, представленных рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, эти нормативные рамки также были одобрены.

В прошлом году Ирландия обнародовала свою национальную позицию в поддержку применения международного права в киберпространстве — одного из четырех компонентов нормативных рамок. Ирландия готова сотрудничать с другими государствами — членами Европейского союза и международными партнерами, чтобы действовать в соответствии с нормативными рамками и содействовать миру и стабильности путем их внедрения на глобальном уровне.

Ирландия считает, что внедрение и совершенствование нормативных рамок имеют важнейшее значение для поддержания международной безопасности в киберпространстве и поэтому должны занимать центральное место в любом механизме, предусматривающем проведение регулярного институционального диалога. В предлагаемом будущем механизме поддержания регулярного институционального диалога, который может быть создан по окончании работы нынешней рабочей группы открытого состава, как это предусмотрено, в частности, в предложениях о программе действий, признается, что нормативные рамки имеют решающее значение, и предусматривается проведение периодических обзорных конференций для анализа этих рамок.

Ирландия неизменно и всецело поддерживает применение особого подхода к регулярному институциональному диалогу по вопросам безопасности ИКТ, провозглашенному в программе действий, которая предусматривает создание инклюзивного и ориентированного на конкретные действия механизма для

проведения постоянного будущего диалога. Подход, предусматривающий создание программы действий, позволит наладить постоянный, охватывающий все регионы, многосторонний и прозрачный диалог под эгидой Организации Объединенных Наций. Широкая поддержка программы действий, изложенной в резолюциях Первого комитета Генеральной Ассамблеи, неизменно подтверждалась как в ходе обсуждений в рабочей группе открытого состава, так и в ходе голосования широкой и разнообразной по региональному составу группы государств на Ассамблее.

Обеспечение того, чтобы все государства могли использовать преимущества ИКТ, одновременно снижая риски с помощью мер по наращиванию потенциала, является ключевым элементом нормативных рамок и одной из приоритетных задач Ирландии. На государствах лежит обязанность сократить цифровой разрыв и повысить устойчивость к злонамеренной активности с использованием киберсредств.

Резолюция 78/237 Первого комитета, озаглавленная «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», не отражает ни значимости нормативных рамок, ни широкого спектра мнений, высказанных множеством государств-членов, и поэтому Ирландия не смогла ее поддержать. Ирландия не считает, что подход, предложенный в этой резолюции, может удовлетворить потребности большинства государств-членов. Более того, Ирландия пришла к выводу, что эта резолюция может подорвать поэтапный и основанный на консенсусе метод, с помощью которого рабочей группе открытого состава удавалось добиваться прогресса на протяжении последних лет.

Ирландия по-прежнему надеется на создание на основе консенсуса будущего механизма для проведения регулярного институционального диалога до завершения мандата нынешней рабочей группы открытого состава и будет сотрудничать со всеми государствами в целях содействия созданию инклюзивной и ориентированной на конкретные действия модели, которая будет отражать нормативные рамки.

В ходе дискуссий о том, как, в частности, можно применить подход, предусматривающий создание программы действий, были выдвинуты предложения о проведении ежегодных официальных сессий с подробными обсуждениями открытого характера и техническими совещаниями по конкретным стратегическим вопросам в течение года. Технические группы могли бы заниматься такими вопросами, как гендерная проблематика, цифровое неравенство и роль неправительственных организаций в процессе внедрения нормативных рамок. Участие в технических рабочих секциях должно быть добровольным и открытым для всех государств и должно приводить к оперативным выводам, основанным на уроках, извлеченных по итогам внедрения нормативных рамок.

Опираясь на межрегиональную поддержку резолюций Первого комитета, в которых выдвигается подход, предусматривающий создание программы действий, этот конкретный механизм сможет укрепить региональное взаимодействие и сотрудничество с региональными организациями для поддержки усилий по наращиванию потенциала с учетом потребностей.

Обнадеживает то, что предлагаемая программа действий также предусматривает официальное участие соответствующих заинтересованных сторон, включая частный сектор, научные круги и гражданское общество, и регулярные консультации с ними для внесения ими вклада в решение актуальных вопросов. Ирландия решительно выступает за участие многих заинтересованных сторон в регулярном институциональном диалоге, твердо веря, что это позволит более

эффективно сосредоточить усилия на поддержке государств в процессе внедрения нормативных рамок ответственного поведения государств и наращивания потенциала с учетом потребностей для укрепления устойчивости перед киберугрозами.

Для того чтобы к концу срока действия мандата рабочей группы открытого состава наладить полноценный регулярный институциональный диалог, Ирландия поддерживает идею организации межсессионных совещаний и специальных сессий рабочей группы открытого состава в 2024 и 2025 годах, в том числе по вопросу о последствиях для бюджета.

Япония

[Подлинный текст на английском языке]
[30 апреля 2024 года]

1. Введение

Япония поддерживает идею учреждения в качестве будущего механизма программы действий по поощрению ответственного поведения государств в киберпространстве. Япония считает, что программа действий является подходящим форумом для продолжения наших дискуссий об ответственном поведении государств в киберпространстве. Программа действий как ориентированный на практические действия механизм должна служить платформой для поддержки усилий каждой страны по внедрению согласованных норм и принципов ответственного поведения государств путем поощрения обмена передовым опытом и определения конкретных проблем, с которыми сталкивается каждая страна.

Программа действий должна быть единым механизмом последующей деятельности по итогам работы нынешней рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 и начать функционировать для реализации результатов деятельности рабочей группы открытого состава после завершения выполнения ею своего мандата. Программа действий будет учреждена после завершения срока действия мандата нынешней рабочей группы открытого состава и не будет иметь двухвекторного характера.

Япония хотела бы внести максимально возможный вклад в дискуссии, учитывая, что программа действий, следует надеяться, послужит форматом для фактической имплементации согласованных на международном уровне норм и принципов.

Настоящий документ представляет собой обновленный вариант национального вклада Японии, включенного в доклад [A/78/76](#), с учетом прогресса, достигнутого благодаря резолюции [78/16](#) Генеральной Ассамблеи, и продолжения обсуждений в рамках рабочей группы открытого состава 2021–2025.

2. Сфера охвата/цели

Цель программы действий заключается в содействии поддержанию мира и стабильности и поощрении создания открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды.

С учетом этого программа действий должна, в частности, обеспечивать достижение следующих целей:

- a) вынесение рекомендаций, придающих направленность национальным усилиям по внедрению норм и принципов ответственного поведения государства;
- b) поощрение представления добровольной отчетности о национальной практике с целью выявления потребностей и проблем каждого государства-члена;
- c) поддержка наращивания потенциала с учетом потребностей и проблем по просьбе стран — получателей помощи;
- d) общедоступность и широкое участие государств-членов и многих заинтересованных сторон.

Кроме того, программа действий должна быть постоянной платформой для рассмотрения регулярно фигурирующих в повестке дня вопросов путем содействия обсуждению существующих и возникающих угроз, а также вопросов разработки мер укрепления доверия и применимости международного права в киберпространстве.

3. Структура и содержание

a) Структура для содействия имплементации нормативных рамок

При определении сферы охвата, структуры и содержания программы действий в качестве образца можно использовать Программу действий по предотвращению и искоренению незаконной торговли стрелковым оружием и легкими вооружениями во всех ее аспектах и борьбе с ней. Программа действий по стрелковому оружию предусматривает конкретные меры на национальном, региональном и международном уровнях. Затем каждая страна в добровольном порядке представляет доклад о своем правовом и институциональном развитии и других видах практики и проводит ежегодное обзорное совещание.

Добровольно представляемый доклад в рамках программы действий по кибервопросам должен включать протокол проверки хода имплементации норм в каждой стране, в частности хода работы по разработке политики, законов и руководящих принципов по защите критически важной инфраструктуры, и положении дел с реагированием на инциденты в каждой стране или регионе. Было бы целесообразно, если бы каждое государство-член также уточняло и указывало, какого рода потенциал ему необходимо укреплять. Эта работа должна способствовать созданию основы для поддержки национальных усилий по имплементации норм в каждой стране.

Структура и формат программы действий должны предусматривать проведение регулярных пленарных заседаний в Организации Объединенных Наций на ежегодной или двухгодичной основе. В рамках пленарных заседаний по программе действий можно принимать и регулярно обновлять практические рекомендации для выполнения на национальном уровне. Например, на пленарных заседаниях может быть определена приоритетная тема в отношении имплементации нормативных рамок, в частности внедрение той или иной нормы, существующие и возникающие угрозы, защита критически важной инфраструктуры и так далее.

Для поддержки дальнейшего обмена мнениями по этой теме участники пленарных заседаний могут принять решение о создании специальных рабочих секций либо технических совещаний или рабочих групп открытого состава, которые будут проводить межсессионные заседания в рамках пленарных заседаний по программе действий и представлять свои выводы на следующих пленарных заседаниях.

В дополнение к обсуждению дальнейшего совершенствования нормативных рамок в контексте программы действий будут созываться обзорные конференции с периодичностью, которая будет определена с учетом стремительного развития технологий и которая не будет обременительной, особенно для делегаций из развивающихся стран.

Глобальный реестр контактных пунктов, который должен быть создан нынешней рабочей группой открытого состава, станет неотъемлемой частью программы действий в интересах осуществления и дальнейшей доработки мер укрепления доверия.

b) Нарращивание потенциала

Программа действий будет предусматривать поддержку усилий по наращиванию потенциала в связи с имплементацией нормативных рамок, обеспечивая участие многих заинтересованных сторон.

В рамках программы действий будет целесообразно выявить пробелы в потенциале государств-членов в области имплементации нормативных рамок и задействовать существующие инициативы по наращиванию потенциала, чтобы заполнить эти пробелы.

Во время совещаний по программе действий брифинги могут проводить представители других организаций (например, Центра по наращиванию потенциала в области кибербезопасности Ассоциации государств Юго-Восточной Азии и Японии, Международного союза электросвязи и Многостороннего донорского целевого фонда Всемирного банка по кибербезопасности), чтобы обеспечить координацию и взаимодополняемость мероприятий по наращиванию потенциала, проводимых каждой структурой.

Программа действий должна функционировать как платформа под эгидой Организации Объединенных Наций, чтобы обеспечить синергию и задействование усилий, предпринимаемых другими региональными организациями, вместо осуществления программ по наращиванию потенциала самостоятельно.

c) Международное право и нормы

В мае 2021 года Япония представила и опубликовала документ с основной позицией правительства Японии по международному праву, применимому к кибероперациям, и она подтверждает, что действующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, применимо к кибероперациям. В нем изложен ее нынешний подход к применению действующего международного права к кибероперациям, который обобщает взгляды Японии на самые важные и самые фундаментальные вопросы. Япония по-прежнему надеется, что заявление о ее основной позиции в отношении применимости международного права к кибероперациям правительствами различных государств и применения международного права в международных и национальных судах и трибуналах углубит общее понимание международным сообществом порядка применения международного права к кибероперациям в рамках программы действий.

Программа действий также будет поощрять добровольное представление отчетности о национальных усилиях по имплементации нормативных рамок либо путем создания собственной системы отчетности, либо путем содействия использованию существующего механизма (например, национального обзора выполнения рекомендаций Организации Объединенных Наций по ответственному использованию государствами ИКТ в контексте международной безопасности Института Организации Объединенных Наций по исследованию проблем

разоружения или национальных докладов Генеральному секретарю). Эта отчетность послужит основой для определения приоритетов в отношении имплементации нормативных рамок и учета потребностей в области наращивания потенциала.

На пленарных заседаниях по программе действий можно было бы обсудить способы углубления понимания вопросов применения международного права в киберпространстве. Можно также создать специальную рабочую секцию для содействия обмену мнениями о применимости существующего международного права к кибероперациям. Специальные рабочие секции могут задействоваться на основе мандата государств-членов для обмена национальными мнениями и проведения дискуссий на основе анализа сценариев. Такие специальные рабочие секции могут быть посвящены общим вопросам, конкретным концепциям международного права или тематическим вопросам, таким как кибероперации против критически важной инфраструктуры, и при этом охватывать соответствующие принципы международного права.

d) Участие многих заинтересованных сторон

Заинтересованные стороны занимают центральное место в киберпространстве, будь то в качестве владельцев и операторов элементов инфраструктуры или в качестве активных представителей сообществ. Учитывая взаимосвязанный характер киберпространства, важно привлечь к обсуждению в Организации Объединенных Наций сообщество многих заинтересованных сторон.

Программа действий позволит наладить взаимодействие и сотрудничество с сообществом многих заинтересованных сторон, в том числе для проведения наиболее оптимальных мероприятий по наращиванию потенциала.

4. Подготовительная работа и форматы учреждения будущего механизма

Япония поддерживает дальнейшие целенаправленные обсуждения в рамках рабочей группы открытого состава 2021–2025, направленные на доработку будущего механизма.

Латвия

[Подлинный текст на английском языке]
[30 апреля 2024 года]

Вопрос о нормативных рамках ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ) уже давно — с 2003 года — фигурирует в повестке дня Первого комитета Генеральной Ассамблеи и обсуждается в нескольких группах правительственных экспертов, а также рабочих группах открытого состава, что подчеркивает растущее значение ответственного использования ИКТ для поддержания международной стабильности и безопасности. Сотрудничество между государствами имеет жизненно важное значение для эффективного противодействия растущим угрозам в киберпространстве и укрепления доверия между государствами. По этим причинам настало время принять решение о создании в рамках Организации Объединенных Наций постоянного механизма для рассмотрения вопросов, касающихся кибербезопасности, в долгосрочной перспективе.

В современном взаимосвязанном мире кибератаки становятся все более изощренными и разрушительными и случаются чаще, чем когда-либо. Киберландшафт постоянно развивается. Растет число кибератак на крайне важные объекты инфраструктуры, политически мотивированных атак и атак с исполь-

зованием вирусов-вымогателей, а также число случаев злонамеренного использования искусственного интеллекта. Поэтому не вызывает сомнений актуальность кибербезопасности при обсуждении вопросов международной безопасности.

Чтобы противостоять беспрецедентным масштабам злонамеренной активности в киберпространстве, Латвия укрепляет собственную кибербезопасность и повышает уровень устойчивости к потрясениям. Помимо прочего, Латвия организует и проводит операции по поиску киберугроз как на национальном уровне, так и в рамках Европейского союза, а наши государственные учреждения делятся знаниями и опытом с гражданами и государственными и частными организациями. В 2023 и 2024 годах Латвия, как и другие государства — члены Европейского союза, неоднократно публично осуждала злонамеренную активность с использованием киберсредств, в том числе кибератаки, направленные против демократических процессов и институтов.

Предложение о налаживании «регулярного институционального диалога» под эгидой Организации Объединенных Наций ранее обсуждалось в Первом комитете и отмечено в заключительном докладе рабочей группы открытого состава 2019–2021¹. Рабочая группа открытого состава 2019–2021 пришла к выводу о том, что любые будущие механизмы поддержания регулярного институционального диалога должны быть «практико-ориентированным процессом с конкретными целями, который основан на достигнутых ранее результатах и носит инклюзивный, прозрачный, консенсусный и нацеленный на результаты характер»². В ежегодном докладе рабочей группы открытого состава 2021–2025 о проделанной работе за 2023 год государства согласовали общие элементы, в первую очередь — одновекторный, возглавляемый государствами постоянный механизм³.

Растущие киберугрозы требуют, чтобы энергия и ресурсы государств были направлены на укрепление сотрудничества и доверия между государствами в долгосрочной перспективе, а не на обсуждение форм нового механизма, которое проводится каждые несколько лет и чревато фрагментацией будущего прогресса. Латвия, будучи небольшим государством, поддерживает одновекторный подход, который будет способствовать эффективному использованию ограниченных ресурсов.

В ответ на призыв к созданию постоянного механизма для поощрения ответственного поведения государств при использовании ИКТ на основе последовательного и долгосрочного подхода была предложена программа действий⁴. Резолюции Генеральной Ассамблеи 77/37⁵ о программе действий на 2022 год и 78/16⁶ о программе действий на 2023 год получили широкую поддержку со стороны государств в Генеральной Ассамблее, и эта инициатива была разработана на транспарентной, всеохватной и поэтапной основе.

¹ Заключительный доклад рабочей группы открытого состава 2019–2021, пп. 68–74.

² Там же, п. 74.

³ Второй ежегодный доклад рабочей группы открытого состава 2021–2025 о проделанной работе (A/78/265), п. 55 а).

⁴ <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

⁵ Резолюция 77/37 Генеральной Ассамблеи, озаглавленная «Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности».

⁶ Резолюция 78/16 Генеральной Ассамблеи, озаглавленная «Программа действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности».

Программа действий в качестве постоянного механизма Организации Объединенных Наций

Латвия считает, что, приняв резолюции 77/37 и 78/16, Генеральная Ассамблея предоставила эффективный мандат на продолжение усилий по учреждению программы действий. Программа действий должна быть постоянным, инклюзивным, ориентированным на действия, возглавляемым государствами механизмом в Первом комитете и платформой, открытой для участия всех государств. Ее главной целью будет содействие укреплению международного мира и безопасности и предотвращение конфликтов и недопонимания между государствами. В сферу охвата программы действий должны входить вопросы, связанные с использованием ИКТ в соответствии с нормами международного права и реализацией принятых Организацией Объединенных Наций рамок ответственного поведения государств в киберпространстве. Как отмечается в резолюции 77/37 Генеральной Ассамблеи, программа действий будет «учитывать согласованные консенсусом итоги, принятые»⁷ рабочей группой открытого состава 2021–2025.

Стабильность и безопасность в киберпространстве будут обеспечиваться путем поддержки имплементации и дальнейшего совершенствования в случае необходимости нормативных рамок ответственного поведения государств на основе международного права, включая Устав Организации Объединенных Наций во всей его полноте⁸. Как отмечается в докладах Группы правительственных экспертов в 2013, 2015 и 2021 годах и докладах рабочей группы открытого состава за 2021 и 2022 годы, международное право, включая международное гуманитарное право, применимо и имеет существенно важное значение для поддержания мира, безопасности и стабильности в киберпространстве.

В целях содействия имплементации рамок ответственного поведения государств программа действий будет поддерживать соответствующие учитывающие потребности мероприятия по наращиванию потенциала. Важно содействовать коллективным усилиям по наращиванию потенциала, обмениваясь опытом и примерами передовой практики в целях повышения национальной и глобальной устойчивости к киберугрозам.

В рамках программы действий могли бы проводиться ежегодные официальные совещания. В период между официальными совещаниями в рамках программы действий можно работать в технических рабочих группах, которые будут заниматься конкретными вопросами. Например, техническая рабочая группа могла бы изучать вопросы дальнейшего углубления понимания применимости международного права в сфере использования ИКТ. На официальных совещаниях будут приниматься рекомендации, подготовленные техническими рабочими группами. Будущие приоритеты программы действий должны периодически пересматриваться в ходе обзорных конференций.

Эти технические группы могут создаваться и расформировываться по решению, принятому на официальных совещаниях. Технические рабочие группы должны быть инклюзивными и открытыми для всех государств, чтобы национальные эксперты могли участвовать в работе в режиме офлайн или онлайн (гибридный формат). Решения о создании технических групп и методах их работы должны приниматься с учетом возможностей и ресурсов малых государств.

Регулярный и полноценный диалог с заинтересованными сторонами — организациями гражданского общества, частным сектором, научно-академичес-

⁷ Резолюция 77/37 Генеральной Ассамблеи, п. 2.

⁸ Резолюция 76/19 Генеральной Ассамблеи, десятый пункт преамбулы.

кими кругами — крайне важен и должен поддерживаться в программе действий. Их опыт в постоянно эволюционирующей киберсфере бесценен, а их вклад имеет значение для поощрения ответственного поведения государства. Кроме того, сами заинтересованные стороны «обязаны использовать ИКТ таким образом, чтобы не создавать угрозу миру и безопасности», поскольку именно они являются движущей силой развития новых технологий⁹.

В 2024 и 2025 годах на оставшихся совещаниях и межсессионных совещаниях рабочей группы открытого состава 2021–2025 должны быть проведены дополнительные узконаправленные обсуждения, чтобы продолжить разработку различных аспектов программы действий, включая условия ее создания. Программа действий должна начать функционировать после завершения деятельности рабочей группы открытого состава 2021–2025.

Нидерланды (Королевство)

[Подлинный текст на английском языке]
[1 мая 2024 года]

Введение

Нидерланды по-прежнему глубоко обеспокоены растущим риском для международной безопасности и стабильности, экономического и социального развития, а также безопасности и благополучия людей, создаваемым вредоносным использованием информационно-коммуникационных технологий (ИКТ) государственными и негосударственными субъектами. Также отмечается, что различные уровни потенциала в области безопасности ИКТ среди государств могут повысить уязвимость во все более взаимосвязанном мире.

Для решения этих проблем государства в ходе ряда межправительственных процессов разработали кумулятивные и эволюционирующие нормативные рамки ответственного поведения государств при использовании ИКТ в контексте международной безопасности. Генеральная Ассамблея неоднократно одобряла эти нормативные рамки на основании консенсусных резолюций.

Чтобы закрепить эти достижения, Нидерланды подчеркивают необходимость поддержания регулярного институционального диалога после завершения работы нынешней рабочей группы открытого состава по вопросам безопасности в сфере ИКТ и самих ИКТ 2021–2025, учрежденной в соответствии с резолюцией 75/240 Генеральной Ассамблеи. С этой целью Нидерланды поддерживают инициативу по учреждению будущей программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, которую Генеральная Ассамблея приветствовала в своих резолюциях 77/37 и 78/16.

В соответствии с пунктом 8 постановляющей части резолюции 78/237, озаглавленной «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», Нидерланды настоящим представляют информацию о своей точке зрения и об оценках по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, в частности в отношении будущего регулярного институционального диалога по данным вопросам под эгидой Организации Объединенных Наций. Изложенные ниже мнения основаны

⁹ Заключительный доклад рабочей группы открытого состава 2019–2021, п. 10.

ваются на материалах, представленных Нидерландами для доклада Генерального секретаря во исполнение резолюции 77/37 (A/78/76).

В рамках рабочей группы открытого состава 2021–2025 был достигнут значительный прогресс в поиске общего мнения о будущем механизме регулярного институционального диалога по вопросам международной безопасности в сфере ИКТ. В этой связи Нидерланды с удовлетворением отмечают общие элементы для регулярного институционального диалога, содержащиеся в ежегодном докладе рабочей группы открытого состава о проделанной работе за 2023 год. Нидерланды по-прежнему привержены достижению дальнейшего прогресса в этом вопросе в рамках рабочей группы открытого состава 2021–2025.

Сфера охвата и цели

Подтверждая пункт 4 постановляющей части резолюции 78/16 Генеральной Ассамблеи, Нидерланды считают, что следует учредить по завершении деятельности рабочей группы открытого состава 2021–2025 и не позднее 2026 года механизм под эгидой Организации Объединенных Наций, который будет постоянным, инклюзивным и ориентированным на практические действия и который будет иметь конкретные цели, как это указано в резолюции 77/37 Генеральной Ассамблеи, и общие элементы для будущего регулярного институционального диалога, согласованные консенсусом в ежегодном докладе рабочей группы открытого состава 2021–2025 о проделанной работе за 2023 год.

Нидерланды поддерживают инициативу по разработке под эгидой Организации Объединенных Наций программы действий по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Программа действий должна основываться на общих элементах для будущего регулярного институционального диалога, согласованных консенсусом в ежегодном докладе рабочей группы открытого состава о проделанной работе за 2023 год, и основывать решения, касающиеся сферы охвата, структуры, содержания и условий, на согласованных консенсусом итогах работы рабочей группы открытого состава 2021–2025.

Структура и деятельность

Нидерланды разделяют мнение о том, что программа действий должна носить всеохватный, транспарентный, консенсусный и нацеленный на результат характер. Мандат программы действий может вытекать из учредительного документа, подтверждающего политическое обязательство государств руководствоваться нормативными рамками ответственного поведения государств в киберпространстве и создающего механизм для дальнейшей реализации его целей.

Программа действий должна быть открытой для участия всех государств — членов Организации Объединенных Наций, постоянных наблюдателей, межправительственных и других организаций и специализированных учреждений. Хотя государства несут главную ответственность за поддержание международного мира и безопасности, программа действий должна также предусматривать возможность конструктивного участия, в том числе в официальных мероприятиях, соответствующих неправительственных заинтересованных сторон, включая частный сектор, академические круги и гражданское общество.

Структура программы действий могла бы предусматривать:

а) проведение периодических обзорных конференций для оценки меняющейся ситуации с киберугрозами и инициатив, реализуемых в рамках программы действий, для обновления рамок по мере необходимости и для обеспечения стратегического руководства;

б) проведение пленарных дискуссий открытого состава для обсуждения существующих и новых угроз, дальнейшего обсуждения применения норм международного права, обсуждения принятия мер по укреплению доверия, определения приоритетов в области наращивания потенциала и рассмотрения хода имплементации норм, правил и принципов, а также для выработки рекомендаций для технических совещаний открытого состава и практических инициатив;

с) проведение технических совещаний открытого состава и/или создание рабочих групп для проведения дискуссий, ориентированных на конкретные действия, открытых для участия соответствующих заинтересованных сторон и посвященных конкретным вопросам.

Подготовительная работа и формы учреждения программы действий

В резолюции 78/16, резолюции 77/37 и докладе Генерального секретаря (A/78/76) содержится первоначальная «дорожная карта» для учреждения программы действий. В 2025 и 2026 годах после завершения деятельности рабочей группы открытого состава, как предполагают Нидерланды, можно провести международную конференцию, открытую для участия неправительственных заинтересованных сторон, которая будет опираться на результаты проделанной подготовительной работы, в том числе рабочей группы открытого состава 2021–2025, для принятия учредительного документа и/или политической декларации.

Наращивание потенциала в рамках будущего механизма

Без ущерба для результатов деятельности рабочей группы открытого состава и решений Генеральной Ассамблеи о создании будущего механизма Нидерланды предлагают следующие элементы для содействия наращиванию потенциала в области кибербезопасности в целях ускорения реализации эволюционирующих и кумулятивных рамок и укрепления международного сотрудничества в этой области. Это предложение основано на цикле, состоящем из четырех этапов:

а) обмен мнениями об угрозах посредством обмена техническими знаниями об угрозах и рассмотрения способов борьбы с ними через призму консенсуса в отношении ответственного поведения государств в киберпространстве;

б) проведение самооценки потребностей в потенциале посредством представления добровольной отчетности на основе кумулятивных и эволюционирующих рамок ответственного поведения государств. Можно использовать существующие методы добровольной отчетности, например проводимый ЮНИДИР обзор хода реализации на национальном уровне рекомендаций Организации Объединенных Наций по ответственному использованию государствами ИКТ в контексте международной безопасности (мексикано-австралийская инициатива);

с) увязка потребностей с ресурсами. Будущий механизм мог бы играть роль платформы для созыва совещаний. Кроме того, принимая во внимание универсальный характер и признание Организации Объединенных Наций, Секретариат Организации Объединенных Наций мог бы играть определенную роль в содействии координации работы организаций и структур по наращиванию потенциала в области кибербезопасности. Будущий механизм мог бы использовать существующие ресурсы, такие как платформа “Cybil Portal” Глобального форума по обмену опытом в области компьютерных технологий, а также, возможно, предложения, рассматриваемые в настоящее время рабочей группой открытого состава 2021–2025, такие как каталог инструментов по наращиванию

потенциала и глобальный портал сотрудничества в области кибербезопасности, предложенные государствами-членами;

d) создание системы обратной связи, с помощью которой государства могли бы обмениваться опытом в своих имплементационных усилиях и деятельности по наращиванию потенциала в области кибербезопасности, что могло бы послужить основой для дальнейших обсуждений использования государствами ИКТ в контексте международной безопасности.

Усилия по наращиванию потенциала в рамках будущего механизма должны предприниматься в соответствии с принципами наращивания потенциала, согласованными в ежегодном докладе рабочей группы открытого состава о проделанной работе за 2023 год.

Новая Зеландия

[Подлинный текст на английском языке]
[30 апреля 2024 года]

1. Кибербезопасность является предметом обсуждения государств под эгидой Организации Объединенных Наций уже более 20 лет. Сменявшие друг друга рабочие группы — группы правительственных экспертов и рабочие группы открытого состава — позволяли проводить регулярный обмен мнениями по вопросам, касающимся кибербезопасности в контексте международной безопасности.

2. Эти рабочие группы достигли важных основополагающих результатов, которые в совокупности способствуют международной безопасности и стабильности благодаря созданию нормативных рамок ответственного поведения государств в киберпространстве, которые были одобрены Генеральной Ассамблеей Организации Объединенных Наций и основаны на четырех принципах:

- международное право (все государства — члены Организации Объединенных Наций согласны с тем, что международное право применимо к поведению государств в киберпространстве);
- нормы ответственного поведения государств в Интернете в мирное время;
- меры укрепления доверия в поддержку транспарентности, предсказуемости и стабильности;
- меры укрепления потенциала, имеющие целью обеспечить, чтобы все государства могли снизить уровень рисков, связанных с расширением возможностей подключения к Интернету, и в то же время получать от этого пользу.

3. Новая Зеландия всецело поддерживает решение Генеральной Ассамблеи, принятое в резолюции 78/16, учредить по завершении деятельности рабочей группы открытого состава 2021–2025 и не позднее 2026 года механизм под эгидой Организации Объединенных Наций, который будет постоянным, инклюзивным и ориентированным на практические действия и который будет иметь конкретные цели, как это указано в резолюции 77/37 Генеральной Ассамблеи, и общие элементы для будущего регулярного институционального диалога, согласованные консенсусом в ежегодном докладе рабочей группы открытого состава 2021–2025 о проделанной работе за 2023 год.

4. Мы предполагаем, что этот механизм станет постоянным местом проведения дискуссий по кибербезопасности в контексте международной безопасности в Организации Объединенных Наций по завершении деятельности нынешней рабочей группы открытого состава 2021–2025 и на основе предложения, принятого в резолюциях Организации Объединенных Наций 77/37 и 78/237. Мы с

удовлетворением отмечаем и поддерживаем резолюцию, которая была представлена Францией от имени межрегиональной группы и которая обеспечивает четкий и транспарентный путь для всех государств к рассмотрению сферы охвата, структуры, содержания и условий работы будущего механизма так, чтобы они дополняли деятельность нынешней рабочей группы открытого состава. В связи с этим мы поддерживаем учреждение программы действий, которая:

а) станет единственным постоянным механизмом для обсуждения вопросов кибербезопасности в Организации Объединенных Наций после 2025 года, обеспечивающим предсказуемость и институциональную стабильность. Согласование форм постоянного механизма также обеспечит долгосрочную эффективность. Неоднократное рассмотрение и согласование форматов работы ряда рабочих групп требовало длительных и неоднократных переговоров, отвлекая от важных обсуждений по существу;

б) будет опираться на согласованные нормативные рамки ответственного поведения государств в киберпространстве, включая обязательства по международному праву и международному гуманитарному праву, обеспечивая, чтобы программа действий основывалась на результатах и способствовала продвижению первоначальной работы, проделанной несколькими группами правительственных экспертов и рабочих групп открытого состава по поощрению ответственного поведения государств в Интернете;

в) будет гарантировать участие различных заинтересованных сторон, в том числе правительств (которые несут ответственность за международный мир и безопасность в киберпространстве), компаний, гражданского общества, технических экспертов, ученых и других организаций, которые вносят свой вклад в создание свободного, открытого, безопасного и функционально совместимого Интернета. Новая Зеландия поддерживает формат, который предусматривает участие (включая заявления и представление письменных докладов) неправительственных заинтересованных сторон в обсуждениях, в том числе в любых официальных и неофициальных совещаниях и обзорных конференциях;

г) будет ориентированной на практические действия, в том числе на практические меры по содействию реализации нормативных рамок ответственного поведения государств и поощрение мер по наращиванию потенциала в поддержку усилий государств по имплементации нормативных рамок и механизмов подотчетности и контроля;

е) будет гибкой и способной к адаптации, чтобы иметь возможность реагировать на возникающие угрозы.

Российская Федерация

[Подлинный текст на русском языке]
[9 апреля 2024 года]

Концептуальный документ о постоянной рабочей группе открытого состава с функцией принятия решений по вопросам безопасности в сфере использования ИКТ и самих ИКТ

Соавторы: Республика Беларусь, Буркина-Фасо, Республика Бурунди, Боливарианская Республика Венесуэла, Республика Зимбабве, Корейская Народно-Демократическая Республика, Республика Куба, Республика Мали, Республика Союз Мьянма, Республика Никарагуа, Российская Федерация, Сирийская Арабская Республика, Республика Судан, Государство Эритрея

Дискуссии в рамках Рабочей группы открытого состава Организации Объединенных Наций по вопросам безопасности в сфере использования информационно-коммуникационных технологий (ИКТ) и самих ИКТ 2021–2025 продемонстрировали запрос мирового сообщества на создание единого постоянно действующего механизма принятия решений по данной проблематике под эгидой Организации Объединенных Наций. Исходим из того, что Рабочая группа открытого состава, на практике доказавшая свою эффективность и востребованность, является оптимальным форматом такого механизма.

Мандат будущей постоянной рабочей группы открытого состава с функцией принятия решений должен быть ориентирован на дальнейшее содействие созданию открытой, безопасной, стабильной, доступной, мирной среды ИКТ через практическую реализацию достигнутых в рамках Рабочей группы открытого состава 2021–2025 договоренностей. Вопросы, входящие в мандат:

- продолжение выработки юридически обязывающих правил, норм и принципов ответственного поведения государств и формирование эффективных механизмов их выполнения как элементов будущего универсального договора об обеспечении международной информационной безопасности;
- выработка общего понимания того, как международное право применяется в сфере использования ИКТ и как действующие нормы могут быть адаптированы с учетом специфики информационного пространства (трансграничность, анонимность, возможность внедрения скрытых функций);
- выработка и реализация мер укрепления доверия и механизмов практического сотрудничества государств, в том числе через установленные каналы взаимодействия уполномоченных структур/органов и глобальный межправительственный реестр контактных пунктов, в целях противодействия угрозам информационной безопасности в сфере использования ИКТ и самих ИКТ и предотвращения межгосударственных конфликтов в глобальном информационном пространстве;
- формирование механизмов/программ оказания содействия государствам в повышении возможностей защиты их национальных информационных ресурсов с учетом конкретных потребностей.

В основе деятельности будущей постоянной рабочей группы открытого состава должны лежать следующие принципы:

- открытость, всеохватность, демократичность, прозрачность;
- ведущая роль государств в содействии диалогу по вопросам безопасности в сфере использования ИКТ государствами под эгидой Первого комитета Генеральной Ассамблеи Организации Объединенных Наций;
- соответствие принципам Устава Организации Объединенных Наций (суверенное равенство государств, неприменение силы и угрозы силой, мирное разрешение международных споров);
- принятие любых решений консенсусом исключительно государствами;
- нецелесообразность дублирования международных усилий по обеспечению безопасности в сфере использования ИКТ и самих ИКТ в рамках нескольких переговорных площадок Организации Объединенных Наций;
- преемственность в отношении консенсусных наработок и рекомендаций предыдущих профильных рабочих групп открытого состава и групп правительственных экспертов;

- гибкость и возможность эволюционного развития по мере изменения потребностей государств и появления новых задач в области обеспечения безопасности в сфере использования ИКТ.

Процедурные вопросы:

- любые решения в постоянной рабочей группе открытого состава утверждаются консенсусом государств (данный параметр должен быть четко прописан в резолюции Генеральной Ассамблеи Организации Объединенных Наций о создании постоянной рабочей группы открытого состава);
- график работы: постоянная рабочая группа открытого состава должна начать работу по завершении деятельности текущей Рабочей группы открытого состава, проводить по две официальные сессии в году в Центральных учреждениях Организации Объединенных Наций в Нью-Йорке (представлены все без исключения государства-члены);
- форма отчетности: доклады Генеральной Ассамблеи Организации Объединенных Наций о проделанной работе, принимаемые консенсусом раз в два года;
- структура: по мере необходимости государства — члены Организации Объединенных Наций могут принять решение о создании вспомогательных подгрупп для более детального, углубленного рассмотрения отдельных аспектов мандата; при этом заседания таких подгрупп не должны происходить одновременно в интересах обеспечения полноценного участия всех делегаций;
- руководство: ведение деятельности постоянной рабочей группы открытого состава осуществляет бюро в составе председателя, двух вице-председателей, докладчика и, при необходимости, председателей подгрупп (также в статусе вице-председателей); состав бюро утверждается государствами раз в два года на основе консенсуса по принципу справедливого географического распределения на ротационной основе от каждой из региональных групп.

Целесообразно в рамках постоянной рабочей группы открытого состава предусмотреть механизм оперативной формализации решений по мере их согласования (по процедуре умолчания с последующим утверждением на очередной сессии). Предпринять практические шаги по поддержанию постоянного информационного обмена между государствами через соответствующий электронный портал.

Представляется полезным предусмотреть взаимодействие постоянной рабочей группы открытого состава с соответствующими региональными организациями и объединениями в формате консультаций ее председателя с группами стран, а также организуемых раз в год межсессионных встреч с их представителями.

Участие негосударственных субъектов (неправительственные организации, деловые круги и научно-академическое сообщество) в работе постоянной рабочей группы открытого состава должно носить сугубо консультативный, неформальный характер: например, в формате проводимых один раз в год межсессионных встреч. Право на присутствие на официальных мероприятиях в качестве наблюдателей предоставляется только аккредитованным (согласованным государствами по принципу консенсуса) негосударственным субъектам.

Сингапур

[Подлинный текст на английском языке]
[1 мая 2024 года]

Сингапур по-прежнему привержен открытому и инклюзивному глобальному обсуждению вопросов, касающихся кибербезопасности, и в этой связи мы считаем крайне важным обязательство всех государств вести будущий одновекторный регулярный институциональный диалог. Будущий одновекторный регулярный институциональный диалог имеет решающее значение для содействия всеобщему принятию и признанию кумулятивных и эволюционирующих рамок ответственного поведения государств при использовании информационно-коммуникационных технологий (ИКТ), согласованных всеми государствами-членами в Организации Объединенных Наций с 1998 года, и для обеспечения общей глобальной платформы для дальнейшего совершенствования и реализации этих рамок. В связи с этим важно, чтобы все государства могли сосредоточить свои усилия на единственном процессе, чтобы дискуссии оставались предметными и не подвергались фрагментации. Кроме того, малые и развивающиеся государства с ограниченными ресурсами не смогут на устойчивой основе участвовать в двухвекторных параллельных процессах.

Сингапур считает, что мы должны и далее опираться на четыре общих элемента для регулярного институционального диалога, согласованные во втором ежегодном докладе рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 о проделанной работе ([A/78/265](#), п. 55), в целях укрепления доверия, которое нам необходимо для достижения консенсуса в отношении одновекторного постоянного механизма.

Важно, чтобы государства использовали оставшееся ограниченное время и возможности для выработки в рамках нынешней рабочей группы открытого состава общего видения дальнейших действий для начала регулярного институционального диалога. Приоритетной задачей должно стать достижение консенсуса. В этой связи Сингапур поддерживает предложение Бразилии, внесенное на седьмой основной сессии рабочей группы открытого состава, о введении моратория на внесение резолюций, касающихся безопасности ИКТ, в Первый комитет Генеральной Ассамблеи до тех пор, пока нынешняя рабочая группа открытого состава не завершит свою работу в 2025 году. Мы поддерживаем дальнейшее проведение председателем рабочей группы открытого состава обсуждения путей совершенствования регулярного институционализированного диалога с целью продолжения разработки и уточнения консенсусного предложения по такому диалогу.

В качестве следующего шага мы считаем, что нынешней рабочей группе открытого состава было бы полезно согласовать сферу охвата, структуру, цели и периодичность встреч в рамках будущего механизма. Ответы на эти практические вопросы — логичный путь для доработки общих элементов, согласованных всеми государствами. Кроме того, это даст делегациям, особенно небольшим делегациям с ограниченными ресурсами, предварительную ясность в отношении того, как будет идти работа после 2025 года, что позволит им начать планирование, необходимое для значительной оптимизации их участия. Чтобы обеспечить устойчивую основу для работы одновекторного универсального постоянного механизма, Сингапур подчеркивает, что структура будущего механизма должна быть достаточно широкой и приемлемой, чтобы способствовать продолжающимся и будущим дискуссиям по предложениям и приоритетам всех делегаций. В частности, было бы полезно периодически проводить обзор работы постоянного механизма, чтобы убедиться, что наши подходы соответствуют динамичной обстановке в плане операционных угроз. В этой связи Сингапур поддер-

живает подход и структуру, представленные в подготовленном Председателем дискуссионном документе от 20 февраля 2024 года о проекте элементов для постоянного механизма. Сингапур рассчитывает на конструктивную работу со всеми делегациями по дальнейшей доработке этих проектов элементов с целью их принятия на основе консенсуса в третьем ежегодном докладе нынешней рабочей группы открытого состава о проделанной работе.

Турция

[Подлинный текст на английском языке]
[1 мая 2024 года]

Информационно-коммуникационные технологии стали неотъемлемой частью общества и экономики и оказывают влияние на все аспекты жизни. Эти технологии используются во многих сферах как отдельными людьми, так и государствами. На сегодняшний день навыки государств в части разработки и использования технологий имеют большое значение для развития и роста. Информационные технологии стали основным двигателем развития практически во всех областях — от транспорта до связи, от оборонной промышленности до медицины, от производства до образования и торговли.

Исследования показывают, что в ближайшие несколько лет тенденции в области технологий будут прогрессировать. Среди них выделяются те тенденции, которые могут привести к появлению новых технологических стандартов и сфер деятельности, а также существенно изменить существующие стандарты и сферы. Представляется, что интернет вещей, 5G, большие данные, блокчейн, искусственный интеллект, автономные транспортные средства и умные роботы — это те технологии, которые будут определять наше настоящее и будущее.

С другой стороны, хотя эти технологии открывают перед нами множество возможностей, они также несут в себе риски с точки зрения кибербезопасности. Структура киберугроз становится все сложнее, а их количество растет с каждым днем, при этом имеющиеся данные указывают на то, что в 2022 году по всему миру было зафиксировано свыше 493 миллионов атак с помощью вирусов-вымогателей¹.

Таким образом, кибербезопасность — это обязательное условие здорового развития и интеграции технологий, которое необходимо учитывать на каждом этапе. Наличие уязвимых мест в информационно-коммуникационных системах может стать причиной выхода этих систем из строя, сделать возможным их неправомерное использование или привести к гибели людей, крупным экономическим потерям, нарушению общественного порядка и/или появлению угрозы для национальной безопасности.

Помимо того что обеспечение кибербезопасности необходимо для противодействия угрозам в высокотехнологичных областях, оно важно также с точки зрения обеспечения благосостояния и национальной безопасности государств в силу рисков, которые отсутствие такой безопасности создает для социально-экономической жизни. С учетом всех этих обстоятельств страны тратят огромные средства на кибербезопасность, развивают технологии в области кибербезопасности и направляют свои усилия на обеспечение безопасности в киберсреде и повышение устойчивости к атакам.

В нашей стране борьба с киберугрозами возведена в ранг национальной политики. В этом контексте Министерство транспорта и инфраструктуры и

¹ www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide.

Агентство информационно-коммуникационных технологий проводят исследования, посвященные обеспечению национальной кибербезопасности, на стратегическом и техническом уровнях соответственно. Кроме того, свой вклад в эти исследования вносят также другие учреждения и организации.

В рамках исследований, которые проводятся начиная с 2012 года, подготавливаются и реализуются национальные стратегии и планы действий в области кибербезопасности. В последнее время в соответствии с Национальной стратегией и планом действий в области кибербезопасности на период 2020–2023 годов проводятся исследования, направленные на обеспечение круглосуточной и ежедневной защиты критически важной инфраструктуры от киберугроз, повышение компетенции групп реагирования на инциденты в киберпространстве, безопасное использование киберпространства всеми социальными группами, поддержание осведомленности о вопросах кибербезопасности на высоком уровне, обмен информацией и сотрудничество с национальными и международными заинтересованными сторонами, а также создание механизмов, предназначенных для гарантирования защиты, предотвращение киберпреступлений и усиление сдерживания.

Кроме того, Министерство транспорта и инфраструктуры приступило к исследованиям с целью подготовить новую стратегию и план действий в области кибербезопасности на период 2024–2028 годов. В этом контексте следует отметить, что благодаря исследованиям продолжает обеспечиваться эффективное сотрудничество всех заинтересованных сторон, расширение сбора и подготовки оперативной информации об угрозах кибербезопасности и обмена такой информацией, повышение уровня готовности страны к инцидентам в киберпространстве, подготовка квалифицированных кадров, развитие инструментов оперативного выявления и раннего реагирования, а также анализ рисков для критически важных секторов и инфраструктуры.

С 2013 года в Турции работу по противодействию инцидентам в киберпространстве координирует Национальная группа реагирования на чрезвычайные ситуации в киберпространстве, входящая в состав Агентства информационно-коммуникационных технологий (TR-CERT). Помимо выявления киберугроз и реагирования на инциденты в области кибербезопасности, в том числе до, во время и после происшествия, TR-CERT отвечает за принятие превентивных мер, направленных на предотвращение и сдерживание угроз в киберпространстве.

Основными направлениями деятельности TR-CERT в области кибербезопасности являются:

- наращивание потенциала в области кибербезопасности;
- принятие мер технологического характера;
- сбор и распространение информации об угрозах;
- защита объектов критически важной инфраструктуры.

Кроме того, в период с 2013 года в рамках работы по укреплению национальной кибербезопасности было создано 14 секторальных групп реагирования на чрезвычайные ситуации в киберпространстве, обслуживающих важнейшие секторы (такие как энергетика, здравоохранение, банковское дело и финансы, управление водными ресурсами, электронные коммуникации и важнейшие государственные услуги) и соответствующие объекты критически важной инфраструктуры, а также более 2200 учрежденческих групп реагирования на чрезвычайные ситуации в киберпространстве. В целях смягчения киберрисков и борьбы с киберугрозами все координируемые TR-CERT группы реагирования на чрезвычайные ситуации в киберпространстве работают круглосуточно и без

выходных. TR-CERT осуществляет мониторинг с помощью инструментов обнаружения и профилактики и поддерживает обмен информацией с соответствующими сторонами с помощью инструментов отчетности. TR-CERT разработала платформу, с помощью которой все действующие в Турции группы реагирования на чрезвычайные ситуации в киберпространстве могут обмениваться информацией, в частности передавать сигналы тревоги, предупреждения и оповещения, касающиеся безопасности, что обеспечивает эффективный и безопасный канал связи.

Еще одним важным элементом укрепления сотрудничества и обеспечения готовности является проведение учений по кибербезопасности. Такие учения, проводимые на национальном и международном уровнях, способствуют усилению защиты киберпространства и проверке мер, которые планируется принять для противодействия потенциальным киберугрозам. Начиная с 2011 года Министерство транспорта и инфраструктуры семь раз организовывало учения по кибербезопасности на национальном уровне и два раза — на международном. Со всем недавно на национальном уровне были проведены учения «Киберщит-2022». По завершении учений «Киберщит-2022» при сотрудничестве Министерства транспорта и инфраструктуры и Агентства информационно-коммуникационных технологий 20 и 21 октября 2022 года были проведены учения «Киберщит-2022 для финансового сектора» с участием государственных учреждений и организаций. В ходе этих учений, организованных с использованием технической инфраструктуры TR-CERT и подготовленных ею сценариев, участники приобрели практический опыт в области кибербезопасности и получили информацию о том, какие шаги необходимо предпринимать в случае потенциальных кибератак. В ближайшем будущем планируется организовать международные учения по кибербезопасности.

Кибербезопасность — это вопрос, который стоит на повестке дня стран всего мира и требует международных усилий. Важную роль в повышении готовности стран противостоять рискам и угрозам в киберпространстве играют сотрудничество на региональном и глобальном уровнях, а также обмен информацией и оперативными данными в области кибербезопасности. В связи с этим Турция развивает двустороннее, региональное и международное сотрудничество по этому направлению; участвует в деятельности международных организаций (таких как Организация Объединенных Наций, Организация Североатлантического договора (НАТО), Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Г-20, Организация экономического сотрудничества и развития, Организация экономического сотрудничества, Группа восьми развивающихся стран, Центр по сотрудничеству в сфере безопасности, Организация тюркских государств и т. д.) по разработке политики и стратегий и вносит вклад в такую деятельность. Кроме того, TR-CERT по-прежнему обменивается оперативной информацией о киберугрозах, участвуя в работе таких международных платформ, как Форум групп оперативного реагирования и обеспечения безопасности, организация «Доверенные инициаторы», Международный союз электросвязи, Альянс по кибербезопасности в интересах взаимного прогресса, Платформа НАТО для обмена информацией о вредоносных программах и Группа реагирования на компьютерные инциденты Организации исламского сотрудничества. Наша страна в качестве страны-спонсора также участвует в работе Центра передового опыта НАТО по совместной киберзащите и является членом учрежденного НАТО механизма оказания поддержки в реагировании на инциденты в киберпространстве. Кроме того, со многими странами Турция подписала меморандумы о взаимопонимании и двустороннем сотрудничестве в области кибербезопасности.

TR-CERT стала участницей созданной организацией «Митре» программы «Широко распространенные факторы уязвимости и подверженности воздействию (CVE)» и в этом контексте присваивает номера CVE уязвимостям программного обеспечения, оборудования и продуктов сторонних производителей и обеспечивает координацию процесса выявления и устранения факторов уязвимости.

Турция является участницей нескольких многосторонних соглашений в области кибербезопасности. Она ратифицировала Конвенцию Совета Европы о киберпреступности (European Treaty Series No. 185). Турция также вносит вклад в исследования, проводимые по линии Специального комитета Организации Объединенных Наций по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Кроме того, Турция является одним из авторов программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности и решительно поддерживает резолюцию 77/37 Генеральной Ассамблеи Организации Объединенных Наций и дальнейшие усилия по учреждению программы действий в качестве постоянного, всеохватного и ориентированного на практические действия механизма.

1. Национальная система кибербезопасности в Турции

Рассматривая вопросы информационной и телекоммуникационной безопасности, в частности вопросы кибербезопасности в Турции, следует отметить, что прогресс в этой области начался еще в 1991 году. Работа Турции по обеспечению кибербезопасности началась с включения киберпреступлений в Уголовный кодекс Турции (Закон № 765) в 1991 году². С тех пор страна достигла значительных успехов в различных аспектах кибербезопасности — одной из ключевых составляющих национальной безопасности. Ниже приведен неисчерпывающий перечень инициатив, реализованных в период до 2012 года.

- В 1999 году в Турции был составлен Генеральный план в отношении национальной информационной инфраструктуры³.
- В 2002 году началось осуществление Плана действий по реализации инициативы «Электронная Турция»⁴.
- В 2003 году было представлено описание проекта «Электронная трансформация Турции» и был намечен краткосрочный план действий на 2003–2004 годы⁵.
- В 2004 году были представлены Закон «Об электронной подписи» (Закон № 5070)⁶ и Уголовный кодекс Турции (Закон № 5237)⁷.
- В 2006 году был опубликован документ «Стратегия и план действий по построению информационного общества на 2006–2010 годы»⁸.

² <https://www.mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf>.

³ http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/991000_TuenaRapor.pdf.

⁴ http://www.bilgitoplumu.gov.tr/Documents/1/Yayinlar/020800_E-TurkiyeEylemPlani.pdf.

⁵ <https://webdosya.csb.gov.tr/db/cbs/icerikler/2005-20180522115122.pdf>.

⁶ <https://kamusm.bilgem.tubitak.gov.tr/dosyalar/mevzuat/kanunlar/kanun.pdf>.

⁷ www.resmigazete.gov.tr/eskiler/2004/10/20041012.htm#1.

⁸ http://www.bilgitoplumu.gov.tr/Documents/1/BT_Strateji/Diger/060500_BilgiToplumuStratejisi.pdf.

- В 2007 году был создан координационный центр турецкой группы реагирования на компьютерные инциденты.
- В 2007 году был принят Закон № 5651 «О правилах публикации в сети Интернет и пресечении преступлений, совершаемых посредством таких публикаций»⁹.
- В 2008 году был введен в действие Закон № 5809 «Об электронных коммуникациях»¹⁰ и одновременно проведены первые национальные учения по кибербезопасности.
- В 2010 году была опубликована Декларация Совета национальной безопасности, в которой признавались глобальный масштаб киберугроз и их последствия для национальной безопасности.
- В том же году Турция присоединилась к Конвенции Совета Европы о киберпреступности (Будапешт, ETS No. 185).
- Принятое Советом министров решение направлять и координировать национальные усилия по обеспечению кибербезопасности привело к созданию в 2012 году Совета по вопросам кибербезопасности¹¹; в том же году под эгидой Совета по научно-техническим исследованиям Турции и Исследовательского центра информатики и информационной безопасности был создан Институт кибербезопасности¹².

Эти знаменательные события отражают существенный прогресс в данной области. Как уже упоминалось выше, 11 июня 2012 года (на тот момент в Турции действовала парламентская система правления) Совет министров утвердил решение об организации, проведении и координации национальных исследований в области кибербезопасности¹³. В соответствии с этим решением был создан Совет по вопросам кибербезопасности¹⁴, а Министерству транспорта, мореходства и связи (в настоящее время — Министерство транспорта и инфраструктуры)¹⁵ было поручено выполнять функции секретариата Совета и координировать деятельность по обеспечению кибербезопасности с соответствующими учреждениями.

За последнее десятилетие темпы развития сектора кибербезопасности Турции заметно ускорились. Среди основных достижений — начало осуществления первой Национальной стратегии и плана действий в области кибербезопасности на период 2013–2014 годов¹⁶, учреждение Национального центра реагирования на инциденты в киберпространстве¹⁷ при Агентстве информационно-коммуникационных технологий¹⁸ и публикация декларации, посвященной созданию, роли и принципам работы групп реагирования на инциденты в киберпространстве¹⁹. Кроме того, в рамках осуществления Национальной стратегии и плана действий в области кибербезопасности на период 2013–2014 годов в государственных учреждениях и организациях были созданы группы реагирования на инциденты в киберпространстве (учрежденческие группы реагирования на

⁹ <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5651.pdf>.

¹⁰ <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5809.pdf>.

¹¹ www.btk.gov.tr/siber-guvenlik-kurulu.

¹² <https://bilgem.tubitak.gov.tr/en/sge/>.

¹³ <https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf>.

¹⁴ www.btk.gov.tr/siber-guvenlik-kurulu.

¹⁵ www.uab.gov.tr/.

¹⁶ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf>.

¹⁷ www.usom.gov.tr/.

¹⁸ www.btk.gov.tr/.

¹⁹ www.usom.gov.tr/hakkimizda.

инциденты в киберпространстве, секторальные группы реагирования на инциденты в киберпространстве). Группы реагирования на инциденты в киберпространстве — это учрежденческие и секторальные структуры, уполномоченные оперативно выявлять угрозы и прогнозировать потенциальные атаки в киберпространстве, а также разрабатывать меры для решения проблем, обусловленных подобными атаками, и информировать о таких мерах. Таким образом, предназначение этих групп заключается в развитии у учреждений и организаций навыков реагирования на происшествия в киберпространстве. В настоящее время Национальный центр реагирования на инциденты в киберпространстве координирует работу 14 секторальных групп реагирования, а над обеспечением безопасности киберпространства Турции усердно трудятся свыше 2100 учрежденческих групп реагирования.

Центр киберзащиты, созданный в составе турецких вооруженных сил в 2012 году, с тех пор был преобразован в Штаб киберзащиты. Департамент по борьбе с киберпреступлениями, который был создан в составе Генерального управления по вопросам безопасности в 2011 году, также позднее подвергся реструктуризации (в 2013 году).

Закон № 6518²⁰, опубликованный в 2014 году, ввел в действие некоторые положения в области кибербезопасности через включение новых статей в Закон № 5809, опубликованный в 2008 году и регулирующий сектор электронных коммуникаций. В соответствии со статьями, включенными в Закон № 5809, под председательством министра транспорта, мореходства и связи был создан Совет по вопросам кибербезопасности, в состав которого вошло высшее руководство государственных учреждений. В соответствии с подпунктом h), добавленным в статью 5 вышеупомянутого закона, на Министерство транспорта, мореходства и связи были возложены обязанности по «определению политики, стратегий и задач, связанных с обеспечением национальной кибербезопасности, подготовке планов действий и проведению образовательных и просветительских мероприятий по вопросам кибербезопасности».

На основании этого нормативного акта Совет по вопросам кибербезопасности был назначен главным органом, ответственным за окончательное утверждение и эффективную реализацию на страновом уровне политики, стратегий и планов действий, разработанных Министерством транспорта, мореходства и связи. Совету также поручено принимать решения по предложениям, связанным с идентификацией объектов критически важной инфраструктуры, и определять учреждения и организации, которые будут освобождены от соблюдения всех или части положений, касающихся кибербезопасности.

В 2016 году были опубликованы Закон № 6698 «О защите персональных данных»²¹ и Национальная стратегия и план действий в области кибербезопасности на период 2016–2019 годов²². Кроме того, в Декрете-законе № 671²³, подготовленном с учетом потребностей того времени, были сформулированы следующие полномочия Агентства информационно-коммуникационных технологий: «Агентство принимает или требует принимать всевозможные меры для защиты государственных учреждений и организаций, физических и юридических лиц от кибератак и обеспечивать сдерживание этих атак». Далее, в 2017 году, при координации со стороны Управления оборонной промышленности (в настоящее время — Секретариат оборонной промышленности²⁴) было начато форми-

²⁰ www.resmigazete.gov.tr/eskiler/2014/02/20140219-1.htm.

²¹ <https://kvkk.gov.tr/Icerik/6649/Personal-Data-Protection-Law>.

²² <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf>.

²³ www.resmigazete.gov.tr/eskiler/2016/08/20160817-18.htm.

²⁴ www.ssb.gov.tr/Default.aspx?LangID=2.

рование Турецкого кластера кибербезопасности, завершены назначения в Совет по защите персональных данных и стартовала деятельность Совета.

В 2018 году вслед за публикацией Декрета-закона № 703 Совет по вопросам кибербезопасности был упразднен²⁵. Было объявлено, что обязанности и мандат Совета будут переданы «совету или органу, который будет назначен президентом». Вместе с тем, несмотря на некоторые частичные назначения, связанные с исполнением этих обязанностей, ни одна из них до сих пор не была официально передана какому-либо совету или органу. С переходом на президентскую систему правления процесс разработки политики претерпел некоторые изменения. Полномочия по выработке политики были переданы президенту Республики. Формулировать и разрабатывать политику было поручено советам по политике (Указ Президента № 1²⁶, ст. 20–22), в то время как за ее реализацию отвечают министерства.

В соответствии с Указом Президента № 1 «О системе президентского правления» от 10 июля 2018 года обязанность «разрабатывать предложения в отношении политики и стратегий в области кибербезопасности» была возложена на Совет по вопросам безопасности и внешней политики при Президенте (Указ Президента № 1, статья 36/1/ğ). Указом Президента № 1 ответственность за «разработку проектов, посвященных укреплению информационной безопасности и кибербезопасности» была возложена на Управление цифровой трансформации при Президенте Турецкой Республики²⁷, и в частности на Департамент по вопросам кибербезопасности²⁸ при Управлении цифровой трансформации. Обязанности Департамента включают:

- разработку стратегий обеспечения кибербезопасности для государственных учреждений и объектов критически важной инфраструктуры в соответствии с утвержденной президентом политикой;
- мониторинг тенденций для эффективной реализации общенациональных политики, стратегий и планов действий в области кибербезопасности;
- проведение исследований для идентификации объектов критически важной инфраструктуры;
- активизацию сотрудничества между государственным и частным секторами и университетами для формирования национальной экосистемы кибербезопасности;
- проведение исследований в целях разработки местных и общенациональных продуктов в области кибербезопасности во всех секторах, особенно в секторе критически важной инфраструктуры, и пропаганду их использования в государственном секторе;
- проведение мероприятий по предупреждению и защите для обеспечения безопасности критически важных технологий и сохранности информационных активов;
- проведение исследований, посвященных созданию системы информационной безопасности и управлению ею в государственных учреждениях и организациях, эксплуатирующих объекты критически важной инфраструктуры, что предполагает установление технических стандартов и процедур,

²⁵ <https://www.resmigazete.gov.tr/eskiler/2018/07/20180709M3-1.pdf>.

²⁶ <https://www.mevzuat.gov.tr/mevzuatmetin/19.5.1.pdf>.

²⁷ <https://cbddo.gov.tr/en/>.

²⁸ <https://cbddo.gov.tr/en/department-of-cyber-security/>.

а также принципов мониторинга работы приложений и управления их работой.

Кроме того, в соответствии с Указом Президента № 1, опубликованным в «Официальном вестнике» от 10 июля 2018 года, при Министерстве промышленности и технологий²⁹ был создан Национальный технологический директорат³⁰. На Директорат были возложены следующие обязанности по обеспечению кибербезопасности:

- повышение уровня кибербезопасности и информационной безопасности информационных технологий, а также передовых технических продуктов и систем;
- разработка местных и общенациональных продуктов в области кибербезопасности;
- расширение использования местных и общенациональных продуктов по всей стране;
- совершенствование инфраструктуры центров хранения и обработки данных;
- поддержка экосистемы кибербезопасности через различные программы стимулирования.

Резюмируя вышеизложенное, следует отметить, что в соответствии с различными законами, инструкциями и другими нормативно-правовыми актами задачи по надзору за обеспечением национальной кибербезопасности возложены на ряд учреждений. Их обязанности, связанные с кибербезопасностью, определены в таких различных законодательных актах. Как и в большинстве других стран, обеспечение кибербезопасности в Турции считается общей ответственностью множества государственных структур. Управление цифровой трансформации и Министерство транспорта и инфраструктуры ведут исследовательскую деятельность, связанную с разработкой стратегий и политики в области кибербезопасности. Каждая организация обладает собственным набором функций и обязанностей в сфере своей компетенции.

2. Функции и обязанности Управления цифровой трансформации в области кибербезопасности

Вслед за переходом на президентскую систему правления в 2018 году в соответствии с Указом Президента № 1, который вступил в силу после публикации в «Официальном вестнике» от 10 июля 2018 года, было создано Управление цифровой трансформации при Президенте Турецкой Республики. Впоследствии мандат Управления цифровой трансформации был расширен Указом Президента № 48, опубликованным 24 октября 2019 года³¹.

Создание Управления цифровой трансформации ознаменовало новую эру усилий по цифровизации в Турции и стало свидетельством изменения представлений о такой работе. С момента его создания началось формирование более последовательного и комплексного межучрежденческого подхода к цифровой трансформации в государственном секторе. Соответственно, помимо повышения скорости, транспарентности и эффективности административных процедур, перед Управлением поставлена цель централизованной координации мероприятий в области цифровой трансформации, проводимых отдельно различными

²⁹ www.sanayi.gov.tr/anasayfa.

³⁰ www.sanayi.gov.tr/merkez-birimi/c03f1f3bae27/hakkimizda.

³¹ <https://cbddo.gov.tr/en/governance-and-responsibilities>.

учреждениями, и руководства такими мероприятиями с учетом развития технологий, требований общества и тенденций преобразований в государственном секторе. Кроме того, ему поручено «под одной крышей» координировать — как на стратегическом уровне, так и на практике — деятельность, связанную с кибербезопасностью, национальными технологиями, большими данными и искусственным интеллектом, и обеспечивать эффективную реализацию стратегий первоочередной важности. Таким образом, под надзором Управления цифровой трансформации устанавливаются макроцели и реализуются инициативы по защите цифровой инфраструктуры Турции и превращению ее в кибердержаву, обладающую высоким потенциалом сдерживания.

Ниже перечислены функции Управления цифровой трансформации в области кибербезопасности, к которым относятся, помимо прочего, разработка политики и нормативных положений, создание экосистемы кибербезопасности, повышение осведомленности населения, наращивание потенциала, укрепление государственной инфраструктуры и разработка стандартов.

- Разработка стратегий кибербезопасности для государственных учреждений и объектов критически важной инфраструктуры в соответствии с определяемой президентом политикой.
- Разработка проектов, способствующих обеспечению национальной кибербезопасности и информационной безопасности.
- Контроль за ходом и эффективностью реализации политики, стратегий и планов действий в области кибербезопасности в масштабах страны.
- Работа по определению объектов критически важной инфраструктуры.
- Подача предложений в соответствующие ведомства о том, чтобы полностью или частично освободить те или иные учреждения и организации от соблюдения положений, касающихся кибербезопасности.
- Внесение вклада в создание национальной экосистемы кибербезопасности путем расширения сотрудничества между государственным и частным секторами и университетами.
- Определение приоритетных потребностей, связанных с кибербезопасностью, в целях использования возможностей частного сектора в критически важных областях и недопущения дублирования инвестиций.
- Работа по созданию локальных и национальных продуктов в области кибербезопасности во всех сферах, в первую очередь в секторе критической инфраструктуры, и расширение использования такого рода инструментов в государственном секторе.
- Планирование и проведение мероприятий по предупреждению и защите для обеспечения безопасности критически важных технологий и сохранности информационных активов.
- Создание и применение системы управления информационной безопасностью в государственных учреждениях и организациях, эксплуатирующих объекты критически важной инфраструктуры, установление технических стандартов, процедур и принципов, а также мониторинг и направление процесса их соблюдения.

В настоящее время Управление цифровой трансформации является ведущим органом, отвечающим за вопросы кибербезопасности государственных учреждений и критически важных секторов нашей страны. Помимо выполнения функций совета по вопросам кибербезопасности, оно сотрудничает со всеми

учреждениями в целях координации разработки и эффективного претворения в жизнь стратегий и планов действий в масштабах всей страны.

3. Деятельность и проекты Управления цифровой трансформации, связанные с разработкой политики

Несмотря на существование различных толкований концепции кибербезопасности, ей может быть дано следующее простое и всеохватное определение: это дисциплина безопасности, применимая к каждому аспекту работы в киберпространстве и всем компонентам информационных технологий. С учетом того что четвертая промышленная революция, как считается, нацелена на объединение информационных технологий и всех жизненно важных механизмов, ожидается, что дисциплина кибербезопасности станет частью нашей жизненной дисциплины и будет представлять собой одну из мер адаптации к обусловленным этой революцией изменениям в сфере безопасности.

Когда дисциплина безопасности не обеспечивается соответствующим образом, возникают проблемы с безопасностью и конфиденциальностью. Что касается ситуации в рамках всей страны, то на первый план выходят стратегические цели, заключающиеся в защите объектов критически важной инфраструктуры, обеспечении безопасного обмена данными между учреждениями и организациями и обеспечении того, чтобы данные, источник и конечный пользователь которых находятся внутри страны, не попали в другие страны. Еще одна цель заключается в повышении уровня готовности к инцидентам в киберпространстве на институциональном, секторальном и национальном уровнях с помощью подходов, основанных на анализе рисков и планировании с учетом рисков.

Для обеспечения безопасности в цифровом мире правительства разрабатывают и публикуют стратегии обеспечения кибербезопасности, а также гарантируют и контролируют их реализацию, поручая это соответствующим учреждениям. Наша страна также выполняет свой долг в этом отношении. Благодаря соответствующим усилиям нашей страны и координации со стороны Министерства транспорта и инфраструктуры были подготовлены и опубликованы нижеперечисленные стратегии:

- Национальная стратегия и план действий в области кибербезопасности на период 2013–2014 годов³²;
- Национальная стратегия и план действий в области кибербезопасности на период 2016–2019 годов³³;
- Национальная стратегия и план действий в области кибербезопасности на период 2020–2023 годов³⁴.

Упомянутые выше национальные стратегии и планы действий в области кибербезопасности реализуются на основе комплексного и последовательного подхода и предусматривают меры, способствующие обеспечению безопасности новых технологий, которые вошли в нашу жизнь.

Последняя версия Национальной стратегии и плана действий в области кибербезопасности (на 2020–2023 годы)³⁵ была опубликована 28 декабря 2020 года

³² <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/actionplan2013-2014.pdf>.

³³ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/ulusalsibereng.pdf>.

³⁴ <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/national-cyber-security-strategy-2020-2023.pdf>.

³⁵ <https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/national-cyber-security-strategy-2020-2023.pdf>.

при поддержке Управления цифровой трансформации. Она нацелена на поддержку экономического развития нашей страны, защиту социального порядка и национальной безопасности, а также на позиционирование нашей страны в качестве мирового лидера в области кибербезопасности. В этой связи данная стратегия сосредоточена на политике на четырехлетний период, увязана с концепцией кибербезопасности Турции и миссией страны в этом отношении и направлена на дальнейшее приумножение успехов, достигнутых в рамках реализации предыдущих стратегий. Стратегические цели, определенные в Национальной стратегии и плане действий в области кибербезопасности (на 2020–2023 годы), сгруппированы в рамках восьми основных блоков вопросов:

- защита объектов критически важной инфраструктуры и повышение их устойчивости к потрясениям;
- наращивание потенциала на национальном уровне;
- создание органической сети кибербезопасности;
- обеспечение безопасности технологий нового поколения;
- борьба с киберпреступностью;
- развитие и совершенствование общенациональных и местных технологий;
- интеграция аспектов кибербезопасности в систему национальной безопасности;
- наращивание международного сотрудничества.

3.1 Система контроля за осуществлением стратегий и планов действий

Для эффективного руководства осуществлением подготавливаемых президентом стратегий и планов действий и надзора за их осуществлением, а также для руководства деятельностью Турецкого кластера кибербезопасности в рамках Управления цифровой трансформации и надзора за его деятельностью была разработана система контроля за осуществлением стратегий и планов действий. Данная система позволяет отслеживать ход работы и оценивать ее эффективность и достигнутые успехи на основании ранее поставленных задач.

Еще одной функцией Управления цифровой трансформации является оказание содействия в разработке политики при координации со стороны Совета по политике в области науки, техники и инноваций, в том числе оказание содействия в разработке следующих документов:

- проекта национальной политики в области использования технологий, связанных с кибербезопасностью и коммуникационной инфраструктурой;
- проекта национальной политики в области использования технологии 5G и коммуникационных технологий следующего поколения;
- национальной программы действий в отношении технологий кибербезопасности.

3.2 Мероприятия, предусмотренные в Годовой президентской программе на 2023 год

В соответствии с Национальной стратегией и планом действий в области кибербезопасности на период 2020–2023 годов в Годовой президентской

программе на 2023 год³⁶ были предусмотрены следующие мероприятия, за которые Управление цифровой трансформации будет нести непосредственную или косвенную ответственность.

- Будет обновлена Национальная стратегия в области кибербезопасности, доработаны инструкции по обеспечению кибербезопасности и улучшена соответствующая техническая инфраструктура, а также создан надежный координационный механизм.
 - Будет подготовлено рамочное законодательство о кибербезопасности.
 - Будет подготовлена Национальная стратегия и план действий в области кибербезопасности на период 2024–2027 годов.
- Будут определены и внедрены процедуры и принципы создания систем управления информационной безопасностью на объектах критически важной инфраструктуры.
 - Будет обновлено Руководство по информационно-коммуникационной безопасности.
- Для того чтобы оказать благоприятное воздействие на экосистему кибербезопасности и в этой связи создать продукты и инструменты с более высокой добавленной стоимостью, при участии государственных исследовательских институтов и университетов будут разрабатываться проекты, направленные на создание продуктов и технологий в области кибербезопасности, которые в итоге будут передаваться структурам экосистемы кибербезопасности в виде открытого исходного кода.
- Будут прилагаться усилия к укреплению национальной экосистемы кибербезопасности и повышению ее конкурентоспособности на международном уровне.
 - Будет организован международный бизнес-форум на тему кибербезопасности.
 - Заработает платформа для распространения отечественных продуктов в области кибербезопасности, что позволит создать экосистему, способствующую развитию и экспорту востребованных отечественных продуктов в области кибербезопасности.
- В интересах подготовки квалифицированных специалистов по кибербезопасности будут разработаны учебные программы по кибербезопасности для профессиональных колледжей и установлены профессиональные стандарты.
 - Учебные программы профессионально-технических училищ по кибербезопасности — там, где такие учебные программы существуют — будут доработаны.
 - Будут определены названия специальностей выпускников профессионально-технических училищ с учебными программами по кибербезопасности и подготовлены соответствующие стандарты.

³⁶ <https://www.sbb.gov.tr/wp-content/uploads/2022/11/2023-Yili-Cumhurbaskanligi-Yillik-Programi.pdf>.

3.3. Мероприятия, предусмотренные в Годовой президентской программе на 2024 год³⁷

В соответствии с Национальной стратегией и планом действий в области кибербезопасности на период 2020–2023 годов в Годовой президентской программе на 2024 год были предусмотрены следующие мероприятия, за которые Управление цифровой трансформации будет нести непосредственную или косвенную ответственность.

- Будет укреплен потенциал финансовых рынков в области противодействия киберугрозам и повышен уровень их кибербезопасности.
 - Для финансового сектора будет опубликована инструкция об обеспечении национальной кибербезопасности и усилении сдерживания нарушений в киберпространстве.
- Будет поощряться работа по приведению национальных стандартов в области кибербезопасности в соответствие с международными стандартами и поддерживаться участие Турции в совместных международных проектах.
 - С учетом международных стандартов и законодательства Европейского союза будет завершена работа над подзаконным актом о безопасности интернета вещей.
- Для того чтобы гарантировать национальную кибербезопасность, будут изданы нормативные положения, подготовленные с учетом Директивы Европейского союза по сетевой и информационной безопасности, его последних усилий в области кибербезопасности и лучших международных практик.
 - Будет опубликована инструкция об обеспечении национальной кибербезопасности и усилении сдерживания нарушений в киберпространстве.
 - Будет проведен анализ в связи с подготовкой нормативного акта о безопасности интернета вещей.
 - Будут проведены проверки кибербезопасности устройств, подключенных к интернету вещей.
 - Будут определены подзаконные акты, которые необходимо будет принять в связи с готовящимся национальным рамочным законодательством о кибербезопасности.
 - Будет вестись работа в отношении Закона об электронной подписи (Закон № 5070) и других соответствующих законодательных актов, для того чтобы заложить правовую основу для удаленного подписания документов.
 - Будут проводиться информационно-разъяснительные мероприятия, направленные на расширение использования услуги удаленного подписания документов в государственных учреждениях и частном секторе.
- Будет обеспечиваться координация национальных мероприятий в области кибербезопасности на самом высоком уровне и создана эффективная

³⁷ <https://www.sbb.gov.tr/wp-content/uploads/2023/10/2024-Yili-Cumhurbaskanligi-Yillik-Programi.pdf>.

структура координации и управления, которая будет способствовать налаживанию межучрежденческого сотрудничества.

- Будет опубликован отдельный закон на тему кибербезопасности, регулирующий функции, задачи и обязанности национальной системы кибербезопасности.
- Будет координироваться подготовка Национальной стратегии и плана действий в области кибербезопасности на период 2024–2028 годов, а также разработан механизм мониторинга деятельности и мероприятий в цифровой среде.
- Будут приложены усилия к составлению национального плана реагирования на чрезвычайные ситуации и кризисы в области кибербезопасности.
- Будет укреплена сеть обмена оперативной информацией о киберугрозах.
- Процессы сбора оперативной информации о киберугрозах и обмена ею будут усовершенствованы за счет увеличения разнообразия ресурсов и разработки приложений, использующих технологии искусственного интеллекта и анализа больших данных, при этом будут прилагаться усилия для раннего выявления и устранения угроз национальной кибербезопасности.
 - Будет проведен анализ потребностей в ресурсах, необходимых для сбора оперативной информации о киберугрозах.
 - Будет укреплен потенциал для реагирования на инциденты и координации усилий.
 - Будет инициирована работа по проектам в области кибербезопасности, предусматривающим использование технологий искусственного интеллекта и анализа больших данных для обнаружения фишинговых доменов, командно-контрольных центров, осуществляющих атаки с помощью вредоносного ПО, и ботнетов.
- Будут определены и внедрены процедуры и принципы создания систем управления информационной безопасностью на объектах критически важной инфраструктуры.
 - Будет проведен анализ процесса создания системы управления информационной безопасностью на объектах критически важной инфраструктуры.
 - Будут разработаны нормы, касающиеся создания системы управления информационной безопасностью на объектах критически важной инфраструктуры.
- Будут установлены стандарты кибербезопасности в вызывающих обеспокоенность отраслях.
 - Будет проведен обзор системы сертификации, созданной в соответствии с Законом Европейского союза о кибербезопасности, и будут определены стандарты, распространяющиеся на продукты, услуги и процессы в области кибербезопасности.
 - Статьи, относящиеся к отраслевым инструкциям по обеспечению информационно-коммуникационной безопасности, будут включены в Руководство по информационно-коммуникационной безопасности.
 - Будет разработана модель, с помощью которой будут определяться критически важные предприятия, подлежащие проверке на основании

- требований Руководства по информационно-коммуникационной безопасности.
- Будет проведена подготовка к процессу проверки в соответствии с Руководством по информационно-коммуникационной безопасности.
 - Будут проводиться мероприятия по ознакомлению с Руководством по информационно-коммуникационной безопасности.
 - Будет создана инфраструктура для проведения проверок уровня кибербезопасности.
 - Будет проведен анализ текущей ситуации в том, что касается работы центров практики и исследований в области кибербезопасности, испытательных стендов для проверки уровня кибербезопасности и университетских интеграционных лабораторий.
 - Будет расширено использование отечественных продуктов в области кибербезопасности, в первую очередь государственными учреждениями.
 - Будет подготовлена дорожная карта по развитию сектора кибербезопасности и обеспечению его участия в глобальных рыночных отношениях.
 - Будут разработаны программы для подготовки квалифицированных кадров и улучшения карьерных перспектив в области кибербезопасности.
 - Для квалифицированных молодых специалистов будут организованы соревнования по кибербезопасности.
 - Будут вестись сотрудничество и координация в целях определения профессиональных стандартов для сотрудников, работающих в области кибербезопасности.
 - Для того чтобы готовить кадры в соответствии с потребностями сектора кибербезопасности, будут улучшены учебные программы, качество подготовки и условия обучения.
 - Будут проводиться онлайн- и лабораторные учебные занятия по кибербезопасности.
 - Академия Агентства информационно-коммуникационных технологий будет и далее проводить онлайн-учебные занятия по кибербезопасности.
 - Практические учебные занятия по кибербезопасности будут проводиться в Центре киберподготовки FETIH.
 - Будут проводиться исследования, направленные на повышение осведомленности населения о кибербезопасности.
 - Будет осуществляться сбор данных в целях разработки материалов курсов по кибербезопасности для начальных и средних школ.
 - Будут разработаны процесс проверки на предмет соблюдения требований Руководства по информационно-коммуникационной безопасности и учебная программа по вопросам информационной безопасности.
 - Для повышения информированности о кибербезопасности будут организованы такие мероприятия, как семинары, тренинги и конкурсы.
 - Будут укреплены механизмы реализации мер по обеспечению информационной и коммуникационной безопасности и механизмы создания, эксплу-

атации и проверки систем управления информационной безопасностью в государственных учреждениях.

- Будут разработаны подзаконные акты, содержащие процедуры и принципы обеспечения информационно-коммуникационной безопасности.
- Будет проведен обзор законодательства и инфраструктуры, связанных с использованием и мониторингом доменных имен, принадлежащих государственным учреждениям и организациям.

4. Деятельность и проекты Управления цифровой трансформации, связанные с разработкой нормативных актов и руководящих принципов в области кибербезопасности

Управление цифровой трансформации прилагает значительные усилия к тому, чтобы укрепить национальный потенциал противодействия путем принятия мер по защите государственного и частного секторов от киберугроз. Среди основных целей этих усилий — совершенствование нормативных актов и стратегий в области кибербезопасности, создание механизмов проверки, предотвращение возникновения зависимости от поставщиков в случае с объектами критически важной инфраструктуры, обеспечение безопасных технических преобразований и защита данных страны. Ниже приводится краткая информация о некоторых процессах нормотворчества.

- Был подготовлен проект нормативного акта, в котором определяются процедуры и принципы обеспечения безопасности веб-сайтов государственных учреждений и организаций и предоставления поддоменов “gov.tr”.
- Был подготовлен проект нормативного акта об обеспечении информационно-коммуникационной безопасности, в котором приводятся технические требования, касающиеся принятия мер по обеспечению информационно-коммуникационной безопасности. Помимо этого, данный проект нормативного акта содержит положения о создании, внедрении, эксплуатации, проверке и постоянном совершенствовании системы управления информационной безопасностью в целях предупреждения и смягчения рисков для информационной безопасности. Предполагается, что требования, изложенные в данном проекте нормативного акта, будут распространяться на все государственные учреждения.
- В настоящее время ведется подготовка закона о национальной кибербезопасности. Этот закон направлен на решение вопросов регулирования и обеспечения национальной кибербезопасности с помощью уникальной системы управления кибербезопасностью, в которой будут использоваться новейшие технологии и которая позволит повысить национальный потенциал противодействия современным киберугрозам.

В оставшейся части этого раздела кратко описаны инициативы, реализация которых завершена или еще продолжается.

4.1 Президентский циркуляр о мерах по обеспечению информационной безопасности № 2019/12

Расширение масштабов цифровизации информации, облегчение прямого доступа к ней, цифровизация инфраструктуры и увеличение числа систем управления информацией несут в себе серьезные риски с точки зрения безопасности. В связи с этим был опубликован Президентский циркуляр о мерах по

обеспечению информационной безопасности № 2019/12³⁸, нацеленный на уменьшение возникающих рисков в сфере безопасности и обеспечение сохранности важнейших типов данных, утечка или повреждение которых может создать угрозу для национальной безопасности или нарушить общественный порядок. В этом циркуляре приводится 21 базовая мера по обеспечению информационно-коммуникационной безопасности³⁹, которую обязаны применять государственные учреждения и структуры частного сектора, обслуживающие объекты критически важной инфраструктуры. Для того чтобы гарантировать защищенность данных, в президентском циркуляре предпринята попытка обеспечить, чтобы данные, принадлежащие той или иной стране, не выходили за ее пределы. Кроме того, в нем подчеркивается, что одним из основных приоритетов Турции является производство и использование разработанных в стране решений в области кибербезопасности. Наконец, в нем также говорится, что «для того, чтобы смягчить и нейтрализовать риски с точки зрения безопасности, и в первую очередь обеспечить сохранность критически важных данных, при координации со стороны Управления цифровой трансформации должно быть подготовлено Руководство по информационно-коммуникационной безопасности».

4.2 Руководство по информационно-коммуникационной безопасности

Помимо вышеупомянутого Президентского циркуляра о мерах по обеспечению информационной безопасности № 2019/12, в 2020 году был опубликован документ под названием «Руководство по информационно-коммуникационной безопасности»⁴⁰. Основная цель данного руководства — подробно сформулировать меры по обеспечению кибербезопасности, которые позволят гарантировать безопасность критически важных информации/данных и объектов инфраструктуры, в случае с которыми отсутствие такой безопасности может привести к нарушению общественного порядка или создать угрозу национальной безопасности. Это руководство является первым опубликованным национальным справочным документом на эту тему, и в нем подчеркивается необходимость разработки комплексной стратегии обеспечения безопасности, охватывающей все аспекты информационной и коммуникационной безопасности. Оно играет важную роль в укреплении потенциала киберзащиты государственных учреждений и поставщиков услуг критически важной инфраструктуры. Кроме того, как в Президентском циркуляре о мерах по обеспечению информационной безопасности № 2019/12, так и в Руководстве по информационно-коммуникационной безопасности содержится распространяющееся на поставщиков требование подтверждать в заявлении, что их продукты не имеют каких-либо дефектов, позволяющих обходить системы защиты.

4.3 Руководство по проверке информационно-коммуникационной безопасности

Для обеспечения устойчивости достижений, намеченных в Руководстве по информационно-коммуникационной безопасности, Управление цифровой трансформации подготовило и опубликовало в октябре 2021 года Руководство по проверке информационно-коммуникационной безопасности⁴¹, признав тем самым, что обеспечение информационно-коммуникационной безопасности невозможно без эффективных действий по проверке и надзору.

Ожидается, что государственные учреждения, организации и предприятия, предоставляющие услуги критически важной инфраструктуры, будут завершать

³⁸ <https://www.mevzuat.gov.tr/MevzuatMetin/CumhurbaskanligiGenelgeleri/20190706-12.pdf>.

³⁹ <https://cbddo.gov.tr/en/presidential-circular-no-2019-12-on-information-security-measures>.

⁴⁰ <https://cbddo.gov.tr/en/icsguide/>.

⁴¹ <https://cbddo.gov.tr/en/icsguide/>.

свои мероприятия по обеспечению соответствия требованиям в течение срока, указанного в Руководстве по информационно-коммуникационной безопасности, и проводить обзорные проверки не реже одного раза в год с целью убедиться в соответствии осуществляемой ими деятельности и принимаемых ими мер установленным требованиям.

Организации такого рода обязаны не только соблюдать требования Руководства по информационно-коммуникационной безопасности, но и проводить регулярные проверки и оценки того, насколько эффективно применяются меры безопасности и насколько оперативный процесс отвечает соответствующим требованиям. Таким образом, проверки должны проводиться на регулярной основе — как минимум один раз в год — либо службой внутренней проверки, либо аккредитованными сторонними проверяющими компаниями. Правила и процедуры проверок, которые должны проводиться организациями в этой связи, прописаны в Руководстве по проверке информационно-коммуникационной безопасности, опубликованном Управлением цифровой трансформации в 2021 году.

4.4 Программа сертификации лиц/компаний, проводящих проверки в области информационно-коммуникационной безопасности

Программа сертификации лиц/компаний, проводящих проверки в области информационно-коммуникационной безопасности, была разработана для выявления компаний и лиц, обладающих навыками, квалификацией и компетенцией, необходимыми для проведения проверок на соответствие требованиям Руководства по информационно-коммуникационной безопасности. Данная программа реализуется в сотрудничестве с Турецким институтом стандартов и Советом по научно-техническим исследованиям Турции. С 2021 года в рамках Программы сертификации были сертифицированы и допущены к проведению проверок 163 лица и 23 компании.

4.5 Система контроля за соблюдением требований и проведением проверок в области информационно-коммуникационной безопасности

Система контроля за соблюдением требований и проведением проверок в области информационно-коммуникационной безопасности⁴² была разработана и внедрена 4 января 2023 года. Эта система позволяет контролировать результаты проверок в отношении всех организаций, на которые распространяется действие Руководства по информационно-коммуникационной безопасности. С тех пор в данной системе зарегистрировались 2945 пользователей и 1191 организация. Благодаря этой системе организации могут представлять информацию о ходе выполнения требований Руководства по информационно-коммуникационной безопасности и ходе проверок. С помощью этой цифровой платформы можно также отслеживать то, насколько на сегодняшний день системы управления информационной безопасностью организаций отвечают установленным требованиям.

4.6 Проект, посвященный анализу и представлению данных касательно национальной модели управления кибербезопасностью

Реализация проекта, посвященного анализу и представлению данных касательно национальной модели управления кибербезопасностью и инициированного для изучения модели управления кибербезопасностью в Турции, завершилась. В рамках этого проекта был проведен сравнительный анализ моделей разных стран и представлены рекомендации по совершенствованию национальной

⁴² <https://cbddo.gov.tr/en/bigdes/>.

модели. Благодаря этому в Турции была разработана система управления кибербезопасностью.

После завершения проекта, посвященного анализу и представлению данных касательно национальной модели управления кибербезопасностью, 13 декабря 2022 года был организован национальный практикум по кибербезопасности, на котором были представлены результаты проделанной работы. В ходе этого практикума своими мнениями и предложениями поделились свыше 40 государственных учреждений и более 100 участников. Результаты практикума показали, что существует необходимость в разработке закона о национальной кибербезопасности. В настоящее время этот закон находится на стадии окончательной доработки.

5. Деятельность и проекты Управления цифровой трансформации, связанные с экосистемой кибербезопасности

5.1 Турецкий кластер кибербезопасности

В октябре 2017 года государственные учреждения, научные круги и крупнейшие частные компании, занимающиеся вопросами кибербезопасности, были приглашены для обсуждения возможностей для сотрудничества, что привело к созданию Турецкого кластера кибербезопасности⁴³. На сегодняшний день Кластер функционирует при координации со стороны Управления цифровой трансформации и Секретариата оборонной промышленности и насчитывает более 200 участников, которые производят и оказывают свыше 400 продуктов и услуг. Кроме того, с 2018 года Турецкий кластер кибербезопасности является членом Глобального партнерства экосистем инноваций и кибербезопасности (Global EPIC).

Перед Турецким кластером кибербезопасности поставлено несколько целей, включая следующие:

- увеличение числа компаний, занимающихся вопросами кибербезопасности;
- поддержка развития технического, административного и финансового потенциала присоединившихся компаний;
- улучшение брендинга продуктов и услуг;
- улучшение стандартов экосистемы кибербезопасности;
- повышение конкурентоспособности присоединившихся компаний на национальном и глобальном рынках;
- приумножение человеческого капитала в области кибербезопасности;
- повышение осведомленности общества о кибербезопасности.

Хотя частный сектор по закону не обязан принимать участие в такой совместной работе, взаимное доверие и сотрудничество между государственным сектором и частными учреждениями остаются в центре внимания. Основная мотивация соответствующих усилий — укрепление отношений между покупателями и поставщиками, развитие общих каналов сбыта, предоставление площадки для налаживания контактов и совместное ведение научно-исследовательской деятельности университетами и компаниями, что может открыть новые возможности и принести пользу обеим сторонам. Благодаря общим экономическим интересам компаниям, присоединившимся к Кластеру, удалось повысить

⁴³ <https://siberkume.org.tr/>.

свою производительность, укрепить потенциал для инноваций и, как следствие, стать более конкурентноспособными, чем компании, работающие в одиночку.

Как правило, добиться успеха в области кибербезопасности невозможно без поддержки высших органов государственной власти. Некоторые турецкие компании вышли на международный рынок и продают свои качественные и уникальные продукты в области кибербезопасности за рубежом. Некоторые из этих продуктов включены в отчеты компании «Гартнер». В частности, они представлены в категории «Симуляторы взломов и атак».

5.2 Совет по внешнеэкономическим связям — Совет предпринимателей из сферы цифровых технологий — Комитет по кибербезопасности

Для того чтобы повысить эффективность работы наших местных и национальных компаний за рубежом, при поддержке Управления цифровой трансформации и при координации со стороны Совета по внешнеэкономическим связям был сформирован Совет предпринимателей из сферы цифровых технологий⁴⁴, приступивший к работе в июне 2022 года. Совет предпринимателей из сферы цифровых технологий готов реализовывать проекты по следующим направлениям:

- глобализация экосистемы цифровых технологий Турции;
- адаптация к новым тенденциям;
- обеспечение доступа к международному финансированию, цифровые преобразования и нормотворчество.

Перед Советом предпринимателей из сферы цифровых технологий поставлены следующие цели:

- увеличение числа турецких компаний, входящих в список «Форчун-500», и числа турецких компаний-единологов;
- превращение Турции в технологический центр и создание цифровых коридоров в другие страны;
- увеличение экспорта турецкой высокотехнологичной продукции;
- содействие интернационализации технологических компаний с помощью 144 двусторонних деловых обществ Совета по внешнеэкономическим связям;
- содействие цифровой трансформации промышленных предприятий через налаживание партнерских отношений со стартапами;
- увеличение венчурного капитала в секторе как с точки зрения объема капитала, так и с точки зрения количества инвесторов путем создания платформ, объединяющих мировых и национальных венчурных инвесторов, скейлапы и стартапы;
- выявление проблем, с которыми сталкивается сектор, и передача информации об этих проблемах в соответствующие государственные органы.

В состав Совета предпринимателей из сферы цифровых технологий входят подкомитеты, работающие по следующим направлениям: облачные технологии, финансовые технологии, мобильные технологии, гейминг, кибербезопасность, технологии программного обеспечения, инновационные технологии, венчурный капитал, медицинские технологии и технология Web3 на основе блокчейна. Как

⁴⁴ www.deik.org.tr/sectoral-business-councils-digital-technologies-business-council?pm=65.

видно из этой структуры, вопросами кибербезопасности занимается отдельный подкомитет, что свидетельствует об использовании секторального подхода.

Развитие отечественных технологий в области кибербезопасности имеет для Турции стратегическое значение и признано вопросом национальной безопасности. Соответственно, особое внимание уделяется созданию надежных и популярных продуктов и услуг, способных конкурировать с зарубежными аналогами. В условиях все большей осведомленности о рисках и угрозах, связанных с данными, мировой рынок кибербезопасности в последнее время переживает значительный рост. По прогнозам, доля рынка, которую занимают продукты и услуги в области кибербезопасности, будет и далее расти.

Турция вносит вклад в развитие этой отрасли экономики, сотрудничая с частным сектором и государственными учреждениями в разработке своих решений и выведении их на глобальный рынок. В этой связи Управление цифровой трансформации прилагает усилия к совершенствованию отечественных технологий в области кибербезопасности. Эти усилия предусмотрены в мандате, который был сформулирован в Указе Президента № 1 и звучит так: проводить исследования в целях разработки местных и общенациональных продуктов в области кибербезопасности во всех секторах, особенно в секторе критически важной инфраструктуры, и пропагандировать их использование в государственном секторе.

Для стимулирования развития отечественной экосистемы кибербезопасности при координации со стороны Управления цифровой трансформации начал применяться системный подход. Этот подход направлен на интеграцию системы стимулирования с системой государственных закупок, оценку качества отечественных продуктов в области кибербезопасности, а также постепенное совершенствование таких продуктов и расширение их использования.

В 2021 году при координации со стороны Управления цифровой трансформации и при руководящей роли Секретариата оборонной промышленности, Министерства промышленности и технологий, Управления государственного снабжения, Агентства государственных закупок и Президиума по стратегии и бюджету была сформирована Внутренняя координационная группа по вопросам киберпространства. Позднее к этой группе присоединились Министерство финансов и казначейства, Совет по научно-техническим исследованиям Турции, Турецкий институт стандартов, оператор «Турксат», Министерство транспорта и инфраструктуры и Агентство информационно-коммуникационных технологий. Основная цель Группы — поощрять использование местных и национальных продуктов в области кибербезопасности во всех секторах, как внутри страны, так и за рубежом, в первую очередь в государственном секторе. Деятельность Группы ведется по пяти основным направлениям: политика, законодательство, стандартизация/повышение качества, стимулирование/поддержка/финансирование и интернационализация.

6. Деятельность и проекты Управления цифровой трансформации, связанные с повышением осведомленности о кибербезопасности

6.1 Соревнования по кибербезопасности в рамках фестиваля «Технофест»

Управление цифровой трансформации осознает, что потребность в знаниях о кибербезопасности и навыках в этой области становится все более насущной в свете того значения, которое придается информационно-коммуникационным технологиям (ИКТ). В связи с этим Управление цифровой трансформации, помимо прочего, организует соревнования, направленные на повышение осведомленности о кибербезопасности. Один из таких выдающихся проектов — проект

под названием «ХакСтамбул». Это известное во всем мире уникальное соревнование проводится в рамках фестиваля авиации, космоса и технологий «Технофест»⁴⁵ с 2018 года. В рамках этого соревнования возможность продемонстрировать свои таланты предоставляется хакерам со всего мира; как правило, соревнование проходит в Стамбуле под названием «ХакСтамбул», однако в 2020 году оно было проведено в Газиантепе под названием «ХакЗевгма». В августе 2022 года Управление цифровой трансформации организовало соревнование под названием «ХакЧерноморье» в Зонгулдаке.

Прием заявок на участие в соревновании «ХакМастерс 2023», который состоялся 23 апреля 2023 года, завершился в марте 2023 года. Финалисты были определены по итогам онлайн-овой «охоты за головами». На финальном этапе, состоявшемся 28 апреля, участникам был предложен сценарий по кибербезопасности умных устройств. Хакеры пытались взломать и захватить системы, отыскивая уязвимости в устройствах «умного дома», мобильных приложениях, используемых для управления ими, и облачной инфраструктуре, получающей данные с этих устройств.

Каждый год в программу соревнования включаются различные концепции, такие как безопасность операционных технологических систем, и различные испытания в области кибербезопасности, такие как «охота за ошибками» или «захват флага». Эти соревнования направлены на повышение осведомленности о кибербезопасности и привлечение новых талантов к работе в этом секторе. Положительным побочным эффектом реализации этого проекта является укрепление репутации Турции как игрока на мировом рынке кибербезопасности.

Прием заявок на участие в соревновании «ХакМастерс 2024»⁴⁶ заканчивается 31 мая 2024 года, а финальный этап соревнования пройдет в августе 2024 года в Стамбуле в рамках фестиваля «Технофест»⁴⁷.

6.2 Конкурс киберразведки⁴⁸

Помимо прочего, Управление цифровой трансформации совместно с соответствующими государственными учреждениями, включая Министерство национального образования и Министерство по делам молодежи и спорта, структурами частного сектора и неправительственными организациями организует несколько лагерей и учебных программ по кибербезопасности, а также испытания в стиле «захват флага». Такие лагеря и учебные программы позволяют вдохновить молодых людей на использование своих талантов в области кибербезопасности. Важно также отметить, что число участников этих мероприятий превысило один миллион человек.

Еще одним ярким мероприятием являются конкурсы киберразведки. Они проводятся в рамках учебно-просветительской деятельности, направленной на увеличение числа лиц, осведомленных в вопросах кибербезопасности, и весьма эффективны в этом отношении. Всего в этих конкурсах приняли участие 1,5 миллиона учеников начальных, средних и старших классов.

Данные конкурсы проводятся в онлайн-овом режиме и организуются отдельно для учеников начальных, средних и старших классов. Вопросы для конкурсов готовятся Управлением цифровой трансформации и дорабатываются при поддержке Министерства национального образования с учетом текущей учеб-

⁴⁵ www.teknofest.org/en/.

⁴⁶ <https://hackmasters.com.tr/>.

⁴⁷ www.teknofest.org/en/competitions/hack-masters/.

⁴⁸ <https://cbddo.gov.tr/en/projects/cyberintelligencecontest/>.

ной программы. Объявления публикуются на страницах Управления цифровой трансформации, Министерства национального образования и платформы ЕВА (образовательная информационная сеть) в социальных сетях. В рамках этого конкурса ученики, давшие наибольшее количество правильных ответов за как можно более короткий срок, получают неанонсированные призы и награды, что мотивирует их продолжать развиваться в этой области.

В 2023 году состоялся четвертый конкурс на знания в области киберразведки. Этот конкурс, впервые организованный в октябре 2020 года при поддержке президента и Министерства национального образования, ориентирован на учеников начальных, средних и старших классов. Конкурс проходил в три этапа: 27 декабря 2023 года — для учеников начальных классов, 28 декабря 2023 года — для учеников средних классов и 29 декабря 2023 года — для учеников старших классов. Для участия в нем зарегистрировались 16 915 учеников начальных классов, 15 955 учеников средних классов и 4528 учеников старших классов.

6.3 Мультфильм «Цифровая команда»⁴⁹

Проведя множество исследований на тему повышения осведомленности о кибербезопасности в национальном масштабе, Управление цифровой трансформации признает необходимость повышения цифровой грамотности даже среди детей, не являющихся пользователями интернета. Речь идет не только о получении научно-технических знаний. Речь идет также о знаниях, навыках и установках, которые позволяют детям уверенно познавать цифровой мир, не подвергая себя опасности. Одним из важных проектов, разработанных с этой целью и ориентированных на детей, является популярный мультипликационный сериал под названием «Цифровая команда». С 2020 года он выходит на турецком телерадиоканале Çocuk («Малыш»). Основная цель этого проекта — повысить уровень цифровой грамотности и осведомленности среди детей. Материалы для десятисерийного сериала «Цифровая команда» разрабатывались в сотрудничестве с Управлением цифровой трансформации. Его серии касаются широкого спектра тем: от правил безопасного поведения детей в интернете до кибербуллинга, от интернет-зависимости до искусственного интеллекта, от интернета вещей до влияния цифровизации на жизнь и национальные технологии.

7. Деятельность и проекты Управления цифровой трансформации, связанные с учебной подготовкой по кибербезопасности

Вне всякого сомнения, одним из важнейших элементов усилий по обеспечению национальной кибербезопасности являются кадровые ресурсы, обладающие достаточными навыками и опытом. Для того чтобы удовлетворить соответствующие потребности нашей страны, Управление цифровой трансформации проводит мероприятия по повышению уровня подготовки имеющихся кадровых ресурсов. Ниже приводятся сведения о некоторых из этих инициатив.

7.1 Средняя школа с уклоном в кибербезопасность, открытая в сотрудничестве с Министерством национального образования Турецкой Республики

Для развития навыков и потенциала в области кибербезопасности в рамках системы формального образования были предприняты конкретные шаги, в частности разработана учебная программа среднего образования, внедренная в 2020 году.

⁴⁹ www.youtube.com/watch?v=YnuLs6GAogM&ab_channel=CBDijitalID%C3%B6n%C3%BC%C5%9F%C3%BCmOfisi.

Министерством национального образования при содействии Турецкого кластера кибербезопасности, Секретариата оборонной промышленности, Управления цифровой трансформации и Стамбульского технопарка была создана первая в Турции средняя школа кибербезопасности — Анатолийская средняя школа с уклоном в кибербезопасность при Стамбульском технопарке. В данной школе, расположенной на территории Стамбульского технопарка, можно пройти обучение в области информационных технологий, управления сетями и кибербезопасности.

С момента своего открытия данная средняя школа с уклоном в кибербезопасность входит в число самых престижных учебных заведений.

7.2 Создание профессиональных колледжей кибербезопасности в сотрудничестве с Советом по вопросам высшего образования Турецкой Республики

Управление цифровой трансформации приступило к реализации нового проекта по подготовке квалифицированных кадров в области кибербезопасности путем дальнейшего совершенствования модели, задействованной в случае с вышеупомянутой средней школой с уклоном в кибербезопасность. Подписание в 2022 году протокола о сотрудничестве между Управлением цифровой трансформации и Советом по вопросам высшего образования⁵⁰ стало первым шагом к созданию профессиональных колледжей кибербезопасности.

Профессиональные колледжи кибербезопасности с учебными программами исключительно в области кибербезопасности открылись в 2023 году. Первый набор в этих учебных заведениях осуществлялся по специальности «Аналитик и оператор в области кибербезопасности»⁵¹. Эту специальность можно получить в четырех крупнейших университетах Турции: Университете Анкары, Эгейском университете, Техническом университете Гебзе и Стамбульском техническом университете.

8. Турция в глобальных индексах

С внедрением цифровых технологий на местном и национальном уровнях кибербезопасность стала для страны не менее важной, чем физическая безопасность. В свете растущей угрозы в обеспечение кибербезопасности в государственном и частном секторах вкладываются достаточные средства. В государственном и частном секторах и военной сфере реализуется множество совместно координируемых проектов; крупные предприятия оборонной промышленности инвестируют в эту область значительные средства; в сфере образования создаются институты, специализирующиеся на вопросах кибербезопасности; с использованием национального потенциала создаются новые продукты и технологии. Благодаря этим усилиям Турция недавно стала одним из мировых лидеров в области кибербезопасности.

Благодаря направленным на достижение этих целей усилиям правительства и государственных органов рейтинг Турции в глобальных индексах кибербезопасности улучшился.

Турция занимает высокое место в Глобальном индексе кибербезопасности, что отражает достижения страны на сегодняшний день.

⁵⁰ <https://cbddo.gov.tr/projeler/siber-myo/>.

⁵¹ <https://cbddo.gov.tr/sss/siber-myo/>.

В Глобальном индексе кибербезопасности, опубликованном Международным союзом электросвязи в 2021 году⁵², Турция поднялась на девять позиций по сравнению с предыдущим годом и заняла одиннадцатое место в мире и шестое место в Европе.

В современной глобальной обстановке ИКТ играют исключительно важную роль. Они являются движущей силой наших обществ, неразрывно связывая хозяйства, правительства и отдельных людей по всему земному шару. Представить себе мир без мгновенной связи, беспрепятственного доступа к информации или возможности вести бизнес в интернете — значит представить себе принципиально иную реальность. ИКТ оказывают заметное влияние на все стороны человеческой жизни: от распространения знаний и оказания медицинской помощи до развлечений и социального взаимодействия. Они расширяют возможности граждан, стимулируют прорывные инновации и способствуют беспрецедентным темпам экономического роста. Кроме того, правительства могут задействовать потенциал ИКТ для повышения степени эффективности, транспарентности и всеохватности оказания услуг и тем самым внести вклад в создание более инклюзивной и надежной демократической системы.

Тем не менее, несмотря на то что такая парадигма связности обладает огромными преимуществами, она сопряжена также с серьезным риском в плане безопасности. По мере неуклонного усиления зависимости человечества от ИКТ растет и его уязвимость. Злоумышленники — от киберпреступников, стремящихся получить личную выгоду, до спонсируемых государством структур с геополитическими целями — используют эту уязвимость для совершения атак на объекты критически важной инфраструктуры и государственные системы, в которых хранятся конфиденциальные данные и личная информация граждан. Глобальная взаимосвязанность объектов инфраструктуры ИКТ порождает сложные отношения взаимной зависимости, при которых брешь в системе безопасности в одном отдаленном уголке мира может иметь каскадные последствия в других местах и потенциально привести к нарушению работы основных служб, вызвать экономические трудности и подорвать доверие населения. Появление новых технологий, таких как искусственный интеллект и интернет вещей, порождает абсолютно новый пласт проблем в сфере безопасности, которые требуют безотлагательного внимания и разработки инновационных решений, поскольку эти технологии часто чреваты новыми векторами атак и трудностями с обеспечением безопасности обширных сетей взаимосвязанных устройств.

В связи с этим крайне важно тщательно выбирать такой путь развития, который будет способствовать поддержанию разумного баланса между использованием огромного потенциала ИКТ и смягчением связанных с ним рисков. Государства должны уделять первоочередное внимание безопасности информационно-коммуникационных технологий и признавать ее императивом национальной безопасности. Это требует комплексного подхода. Первостепенное значение имеет разработка надежных национальных стратегий кибербезопасности, подкрепляющихся прочными государственно-частными партнерствами, что позволит воспользоваться опытом и ресурсами как государственных органов, так и промышленных предприятий.

Не менее важны совместные усилия государственных органов и бизнеса по инвестированию в учебную подготовку по кибербезопасности и просвещение на эту тему граждан и государственных служащих. Такая учебная подготовка должна не только предусматривать получение технических навыков по

⁵² www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

выявлению и смягчению киберугроз, но и способствовать усвоению гражданами правил кибергигиены.

Кроме того, вне всякого сомнения, существенно важно развивать международное сотрудничество по вопросам безопасности ИКТ. В этом контексте большое значение имеет регулярный межучрежденческий диалог под эгидой Организации Объединенных Наций. Государства-члены должны совместно работать над созданием такой системы международных норм, стандартов и правовых рамок, которая будет способствовать ответственному поведению в киберпространстве. Эта система должна предусматривать протоколы обмена информацией для содействия быстрому реагированию на киберугрозы, совместные усилия в области правоприменения для более эффективной борьбы с киберпреступностью и разработку международных договоров, устанавливающих нормы приемлемого поведения в киберпространстве. Цель создания устойчивой инфраструктуры ИКТ предполагает далеко не только принятие оборонительных мер. Ее достижение требует формирования систем, способных не только выдерживать кибератаки, но и быстро восстанавливаться, минимизировать сбои и поддерживать целостность данных. Кроме того, важно содействовать этичному развитию и использованию ИКТ. Государства-члены смогут обеспечить, чтобы эти перспективные технологии служили реализации человеческих ценностей, если будут уделять первостепенное внимание соблюдению конфиденциальности пользователей, пропагандировать ответственный анализ данных, чтобы свести к минимуму возможность злоупотреблений, и обеспечивать прозрачность при разработке и внедрении систем ИКТ.

Если при поощрении инноваций государства-члены будут уделять первоочередное внимание безопасности, они смогут добиться того, чтобы ИКТ и далее играли преобразующую и позитивную роль в формировании нашего мира. Такой совместный подход в сочетании с постоянной бдительностью и адаптацией абсолютно необходим для обеспечения безопасного и процветающего цифрового будущего для всех.

Соединенные Штаты Америки

[Подлинный текст на английском языке]
[1 мая 2024 года]

Введение

Государства — члены Организации Объединенных Наций констатируют, что ИКТ могут использоваться в целях, несовместимых с задачами поддержания международного мира и стабильности. На протяжении многих лет государства собираются под эгидой Организации Объединенных Наций для обсуждения и решения этой проблемы. Путем консенсусного утверждения докладов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 государства выступили за создание нормативных рамок ответственного поведения государств при использовании ИКТ. Эти нормативные рамки, предназначенные для укрепления международной стабильности, включают в себя соответствующие нормы международного права, в частности Устав Организации Объединенных Наций, комплекс необязательных норм и меры укрепления доверия.

Хотя нормативные рамки и получили глобальную поддержку, результаты будут зависеть от соблюдения и имплементации государствами их элементов. В консенсусном докладе Группы правительственных экспертов за 2015 год госу-

дарства впервые утвердили необходимость проведения под эгидой Организации Объединенных Наций регулярного институционального диалога с широким кругом участников¹. Стремясь содействовать прогрессу в этом деле, рабочая группа открытого состава с тех пор неоднократно подтверждала необходимость того, чтобы государства добивались создания механизма для будущего институционального диалога².

Кроме того, как отмечается в самом последнем принятом на основе консенсуса ежегодном докладе о ходе работы рабочей группы открытого состава, государства согласовали первоначальный набор общих элементов регулярного институционального диалога, а также договорились продолжить обсуждение будущей программы действий. Важно, что государства условились, что «в основу будущего регулярного институционального диалога будут положены консенсусные договоренности о рамках ответственного поведения государств»³. Государства условились также, что будущий диалог должен быть одновекторным, возглавляемым государствами и постоянным⁴. Государства заключили, что этот диалог будет представлять собой открытый, инклюзивный, транспарентный, устойчивый и гибкий процесс, который будет адаптироваться по мере необходимости к стремительно эволюционирующим киберугрозам⁵. В своем докладе, опубликованном в апреле 2023 года (A/78/76), Генеральный секретарь подчеркнул настоятельную необходимость учреждения программы и обратил внимание на многие из аспектов, которые были указаны в общих элементах, установленных в ежегодном докладе рабочей группы открытого состава за 2023 год, в том числе на то, что нормативные рамки должны «служить первоосновой» для программы действий⁶. В этом докладе Генеральный секретарь также заключил, что многие государства отмечают ценность инклюзивного и конструктивного участия неправительственных заинтересованных сторон⁷. На официальных и межсессионных совещаниях рабочей группы открытого состава государства продолжали призывать к конструктивному участию множества заинтересованных сторон.

В течение последних двух лет государства пришли к согласию о необходимости учреждения программы действий как будущего постоянного механизма для обсуждения проблем киберпространства в Первом комитете Организации Объединенных Наций. Недавно почти все государства — члены Организации Объединенных Наций проголосовали за резолюцию 78/16; в ней Генеральная Ассамблея решительно учредила механизм, который начнет действовать под эгидой Организации Объединенных Наций по завершении сессии рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

Как указано в резолюции, программа действий будет служить постоянным, но гибким механизмом Организации Объединенных Наций, который будет способствовать функционированию нормативных рамок в целях укрепления мира и безопасности в киберпространстве, в том числе путем конструктивного взаимодействия с сообществом множества заинтересованных сторон и содействия наращиванию потенциала через Организацию Объединенных Наций, которая будет играть роль платформы для обмена информацией.

¹ A/70/174, п. 18.

² A/75/816, пп. 70–74, и A/78/265, п. 52.

³ A/78/265, п. 55 с).

⁴ Там же, п. 55 а).

⁵ Там же, п. 55 d).

⁶ A/78/76, п. 42.

⁷ A/78/76, п. 40.

Сфера охвата программы действий

В резолюции 77/37 Генеральной Ассамблеи сфера охвата и мандат программы действий были определены следующим образом:

[функционировать] «в качестве постоянного, всеохватного, ориентированного на практические действия механизма для обсуждения существующих и потенциальных угроз; поддержки потенциала и усилий государств по осуществлению и продвижению обязательств, касающихся необходимости руководствоваться основой ответственного поведения государств, которая включает в себя добровольные, не имеющие обязательной силы нормы, предусматривающие применение норм международного права к использованию государствами информационно-коммуникационных технологий, принятие мер укрепления доверия и наращивания потенциала, как это указано в резолюции 76/19 Генеральной Ассамблеи, докладах групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы, докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2021 год и первом ежегодном докладе о проделанной работе, представленном рабочей группой открытого состава по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий 2021–2025; обсуждения и, при необходимости, дальнейшего развития этой основы; поощрения взаимодействия и сотрудничества с соответствующими заинтересованными сторонами; периодического обзора прогресса, достигнутого в осуществлении программы действий, а также в дальнейшем функционировании этой программы»⁸.

В резолюции 78/16 Генеральная Ассамблея подтвердила цели программы действий, сформулированные в резолюции 77/37, а также постановила, что механизм будет иметь общие элементы, которые были изложены в докладе рабочей группы открытого состава о проделанной работе за 2023 год. Кроме того, Ассамблея постановила, что сфера охвата, структура, содержание и порядок работы этого механизма должны определяться на основе консенсусных итоговых документов рабочей группы открытого состава.

В резолюциях по программе действий и резолюциях, в которых консенсусом были утверждены доклады Группы правительственных экспертов и рабочей группы открытого состава, государства неоднократно подтверждали, что в своих действиях им следует руководствоваться оценками и рекомендациями групп правительственных экспертов 2010, 2013, 2015 и 2021 годов, рекомендациями Рабочей группы открытого состава 2021 года по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, а также консенсусными документами действующей рабочей группы открытого состава (например, первым и вторым ежегодными докладами о проделанной работе), в частности «кумулятивными и эволюционирующими рамками ответственного поведения государств при использовании информационно-коммуникационных технологий, разработанными и принятыми консенсусом в ходе этих процессов»⁹. Эти консенсусные рамки, сформулированные в принятых консенсусом докладах Группы правительственных экспертов и рабочей группы открытого состава и последовательно одобренные всеми государствами-членами, являются основой программы действий.

⁸ Резолюция 77/37 Генеральной Ассамблеи, п. 26.

⁹ Резолюция 78/16 Генеральной Ассамблеи, восьмой пункт преамбулы.

Государства-члены определяют направленность программы действий и будут обновлять ее, уделяя приоритетное внимание практической имплементации и работе по наращиванию потенциала, ориентированной на внедрение нормативных рамок. Благодаря своему постоянному характеру программа действий будет служить государствам долговременной опорой в этих усилиях.

В качестве постоянного механизма программа действий должна также обладать гибкостью для устранения будущих угроз и оперативностью для оценки меняющихся потребностей государств и освоения их передового опыта борьбы с этими угрозами. В рамках программы действий государства смогут также рассматривать вопрос о том, следует ли менять консенсусные нормативные рамки и каким образом.

В процессе реализации программы действий будут непременно участвовать негосударственные заинтересованные стороны. Почти во всех усилиях по наращиванию потенциала — как международных, так и внутренних — участвуют частный сектор, гражданское общество, академические круги и другие негосударственные заинтересованные стороны. В программе действий для участия заинтересованных сторон должны быть предусмотрены максимально инклюзивные условия, чтобы опыт этих заинтересованных сторон использовался в полной мере.

Учреждение программы действий

Государства-члены должны постараться, чтобы программа действий начала функционировать в 2025 году сразу же по завершении деятельности рабочей группы открытого состава 2021–2025 годов. Такому бесперебойному переходу должен способствовать заключительный доклад рабочей группы открытого состава, где будет подтвержден мандат программы, определенный резолюцией 77/37 Генеральной Ассамблеи и основанный на принятых консенсусом нормативных рамках; где будут сформулированы ее ориентированные на действия структура и методы работы, определены приоритетные направления работы, подтверждены максимально инклюзивный подход к участию заинтересованных сторон и намечены дальнейшие шаги и подробные сроки официального запуска программы к 2026 году.

Для того чтобы полностью определить порядок работы программы действий, может потребоваться дополнительное подготовительное совещание или процесс. Кроме того, если рабочей группе открытого состава не удастся достичь консенсуса по заключительному докладу, то для выполнения содержащегося в резолюции 78/16 решения о запуске программы к 2026 году потребуются провести более широкую «международную конференцию» или другой подготовительный процесс, который будет организован через Генеральную Ассамблею¹⁰. Чтобы обеспечить непрерывность этих важных многосторонних обсуждений, встречи в рамках программы должны начаться в 2026 году.

Учитывая предусмотренную программой действий задачу рассмотрения вопросов мира и безопасности в связи с использованием ИКТ, она, разумеется, должна быть учреждена в рамках Первого комитета. Секретариатом этого будущего механизма было бы логично сделать Управление по вопросам разоружения. Программа действий должна функционировать в максимально возможной степени в пределах имеющихся бюджетных ресурсов.

¹⁰ См. резолюцию 77/37 Генеральной Ассамблеи, п. 3.

Структура

В рамках программы действий должны быть созданы технические рабочие группы, которые будут собираться три-четыре раза в год, и проводиться ежегодные пленарные заседания и периодические обзорные конференции. Программе будет оказывать поддержку секретариатское подразделение в составе Управления по вопросам разоружения.

Технические рабочие группы программы действий являются ее обязательным элементом, обеспечивающим ее ориентированность на действия. Чтобы сделать эти группы как можно более инклюзивными, всем заинтересованным государствам будет предложено совместно готовить в тематических группах конкретные рекомендации, которые будут способствовать имплементации нормативных рамок. Эти рекомендации будут включаться в доклады для рассмотрения на пленарных заседаниях, а затем в Генеральной Ассамблее.

Эти рабочие группы должны быть межрегиональными по составу и применять межсекторальный подход к имплементации нормативных рамок, разрабатывая рекомендации, проводя оценки и формируя свод передовой практики по таким вопросам, как:

- защита критически важных объектов инфраструктуры;
- содействие сотрудничеству между государствами после серьезных киберинцидентов;
- способы усилить ответственность государств за поведение в киберпространстве;
- обмен информацией об эволюционирующих киберугрозах;
- повышение способности государств сдерживать и пресекать угрозы в сфере ИКТ.

Обсуждения конкретных вопросов будут способствовать междисциплинарному предметному обсуждению имплементации нормативных рамок, что позволит выйти за пределы традиционного обособленного подхода, когда угрозы, нормы, вопросы международного права и вопросы наращивания потенциала рассматриваются по отдельности. В рамках рабочей группы открытого состава государства неоднократно подчеркивали, что эти темы перетекают друг в друга и требуют рассмотрения в комплексе. Государства также сходятся в том, что наращивание потенциала затрагивает все остальные темы. Проводимое в рамках рабочих групп по имплементации приоритетное обсуждение потребностей в наращивании потенциала позволит выносить реалистичные и выполнимые рекомендации и ускорить их выполнение.

Ежегодное пленарное заседание должно быть уполномочено оценивать прогресс технических рабочих групп, принимать дальнейшие решения по любым рекомендациям этих групп, обсуждать текущие и назревающие угрозы и рассматривать ход реализации практических инициатив, таких как меры по укреплению доверия. На пленарном заседании могут даваться руководящие указания техническим рабочим группам и по практическим инициативам.

Периодическая обзорная конференция с участием всех государств-членов должна собираться каждые три-четыре года (заменяя ежегодное пленарное заседание в годы проведения конференции), чтобы оценивать эволюционирующие киберугрозы и результаты осуществляемых в рамках программы действий инициатив и деятельности рабочих групп, обновлять нормативные рамки по мере необходимости и определять стратегическое направление работы и мандаты будущих пленарных заседаний, рабочих групп и других инициатив в рамках

программы. Такой регулярный обзор программы позволит государствам адаптировать программу к меняющимся обстоятельствам.

После начала в 2026 году программы действий Первый комитет будет каждый год путем принятия резолюции или решения утверждать все консенсусные решения ежегодных заседаний, проводимых в рамках программы. Первый комитет будет утверждать также итоговые документы обзорных конференций.

Секретариату программы действий, который будет находиться в ведении Управления по вопросам разоружения, будет поручено оказывать поддержку в организации различных совещаний по программе; обслуживать платформы для обмена информацией и механизмы коммуникации и вести архивы; администрировать практические инициативы и проекты, такие как ведение справочника контактных лиц и обеспечение функционирования хранилища угроз и порталов для обмена информацией.

Наращивание потенциала

Учитывая, что страны находятся на разных уровнях развития экспертного потенциала в сфере компьютерных технологий, Организация Объединенных Наций признала, что «наращивание потенциала существенно необходимо для сотрудничества государств и укрепления доверия в области информационно-коммуникационных технологий»¹¹. Организация Объединенных Наций играет существенную роль в созыве совещаний целого ряда заинтересованных сторон, которые активно участвуют в наращивании потенциала для решения соответствующих киберпроблем, и координации и освещении их деятельности, а также в реализации конкретных программ наращивания потенциала по указанию государств-членов.

Предусмотренная программой основная функция наращивания потенциала должна быть непосредственно связана с имплементацией государствами нормативных рамок на национальном уровне. Чтобы обеспечить соответствие деятельности по программе разного рода потребностям государств, в рамках программы действий должны также организовываться специальные обсуждения вопроса о том, какие виды наращивания потенциала нужны государствам для имплементации нормативных рамок. Другими словами, ее целями должны быть повышение осведомленности международного сообщества о важности наращивания киберпотенциала для поддержки имплементации нормативных рамок, содействие координации действий и обмену информацией по имеющимся программам наращивания киберпотенциала с другими заинтересованными сторонами, а также вынесение рекомендаций и ознакомление с передовой практикой, которую государства могли бы внедрить на внутреннем/национальном уровне для имплементации нормативных рамок.

Соединенные Штаты учитывают, что многие государства все еще недостаточно осведомлены о том, что представляют собой нормативные рамки и каково их значение. Кроме того, многие из них не обладают на национальном уровне потенциалом в области кибербезопасности, необходимым для имплементации нормативных рамок; в частности, речь идет о национальных органах и возможностях, связанных с поддержкой реализации норм и мер по укреплению доверия. В Организации Объединенных Наций и вне Организации Объединенных Наций есть целый ряд структур, обладающих экспертным потенциалом в таких областях, как национальная политика и стратегии кибербезопасности, реагирование на киберинциденты и защита критической инфраструктуры, внутреннее законодательство о киберпреступности, культура кибербезопасности, стандарты

¹¹ Там же, двадцатый пункт преамбулы.

кибербезопасности и координация деятельности и подбор доноров для оказания помощи в сфере кибербезопасности на международном уровне. Программа действий не должна дублировать или подменять уже предпринимаемые усилия. Все эти усилия, которые по большей части многосторонни, укрепляют потенциал государств в области национальной безопасности и в конечном итоге способствуют имплементации нормативных рамок, но не входят в мандат программы действий.

Участие многих заинтересованных сторон

Принятие решений в рамках программы действий должно оставаться исключительным полномочием государств. Тем не менее неправительственные заинтересованные стороны, включая гражданское общество, академические круги, региональные и международные органы и частный сектор, играют положительную роль на многосторонних форумах, делясь опытом и знаниями в ходе официальных обсуждений и способствуя наращиванию потенциала. У этих сторон должна быть возможность активно участвовать в программе действий в качестве наблюдателей без права голоса. Опыт и знания неправительственных заинтересованных сторон будут особенно важны в технических и рабочих группах. Эти технические рабочие группы будут способствовать более широкому практическому взаимодействию с рядом неправительственных заинтересованных сторон. Заинтересованные стороны могли бы также представлять периодические отчеты о своих усилиях по реализации инициатив, относящихся к нормативным рамкам, в частности по наращиванию потенциала.

Чтобы программа действий была максимально инклюзивной для заинтересованных сторон, в том числе в рамках ее вспомогательных технических рабочих групп, порядок работы должен основываться на имеющихся эталонных стандартах участия заинтересованных сторон, в частности обеспечивать прозрачность в случае возражений со стороны государств и предусматривать процесс рассмотрения возможности сделать исключение. Например, государства могут взять за образец Рабочую группу открытого состава по проблемам старения. Процедуры этой группы позволяют государствам-членам возражать против участия той или иной организации, но для голосования по вопросу о недопущении организации, против участия которой было высказано возражение, возражения должны высказываться открыто. Организации, против которых в первом раунде не возражает ни одно государство-член, автоматически получают разрешение на участие в официальной сессии¹².

Помимо вопросов аккредитации заинтересованных сторон для участия в совещаниях, проводимых в рамках программы действий, порядок работы должен регулировать и практические аспекты участия аккредитованных заинтересованных сторон в обсуждениях по программе. Здесь за образец можно взять Специальный комитет по разработке всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях. Его процедуры позволяют участие множества заинтересованных сторон, в частности:

- участие в любой открытой официальной сессии;
- в зависимости от имеющегося времени — выступление с устными заявлениями по каждому основному пункту повестки дня по окончании дискуссий государств-членов. Учитывая ограниченность времени, отведенного для заседаний, заинтересованные стороны могут выбрать из своего числа представителей сбалансированным и прозрачным образом, принимая во

¹² См. раздел F документа [A/AC.278/2011/2](#).

внимание принципы справедливого географического представительства и гендерного паритета и многообразие участвующих заинтересованных сторон;

- представление письменных материалов с ограничениями по количеству слов. Эти материалы размещаются на языке оригинала на веб-сайте Специального комитета¹³.

Программа действий должна предусматривать также использование имеющегося на региональном уровне экспертного потенциала и результатов проводимой на этом уровне работы. Предоставление соответствующим структурам возможности участвовать в качестве заинтересованных сторон в обсуждениях, проводимых в рамках программы действий, поможет лучше увязать работу, выполняемую на уровне Организации Объединенных Наций, с региональными усилиями и учитывать конкретные региональные проблемы и обстоятельства.

Венесуэла (Боливарианская Республика)

[Подлинный текст на испанском языке]
[26 апреля 2024 года]

В пункте 8 резолюции [78/237](#) Генеральной Ассамблеи, принятой 22 декабря 2023 года, Ассамблея просила все государства-члены продолжать информировать Генерального секретаря о своей точке зрения и об оценках по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, в частности в отношении будущего регулярного институционального диалога по данным вопросам под эгидой Организации Объединенных Наций, и просила Генерального секретаря представить доклад на основе этих мнений Генеральной Ассамблее в ходе ее семьдесят восьмой сессии для дальнейшего обсуждения государствами-членами на заседаниях Рабочей группы открытого состава в ходе ее восьмой сессии в 2024 году.

В этой связи Боливарианская Республика Венесуэла считает необходимым подчеркнуть важность рабочей группы открытого состава и формата ее работы для выполнения мандата Генеральной Ассамблеи, сформулированного в ее резолюции [75/240](#). Достижения последних лет, такие как создание глобального межправительственного реестра контактных пунктов, свидетельствуют о том, что нынешний формат рабочей группы открытого состава оказался весьма успешным, в частности, благодаря тому, что при принятии решений и утверждении ежегодных докладов она опирается на консенсус.

Боливарианская Республика Венесуэла, подтверждая, что Организации Объединенных Наций следует и далее играть существенно важную и ведущую роль в содействии диалогу по вопросу об использовании государствами информационно-коммуникационных технологий. Особый характер информационно-коммуникационных технологий подразумевает необходимость разработки новых принципов и правил — предпочтительно юридически обязывающих — для устранения несоответствий между существующим международным правом и реалиями виртуальной среды.

В свете вышеизложенного, как представляется, настоятельно необходимо обеспечить преемственность в работе рабочей группы открытого состава 2021–2025, сформировав новую постоянную рабочую группу открытого состава на период после 2025 года, что поможет укрепить потенциал этой новой рабочей

¹³ См. [A/AC.291/6](#), п. 3.

группы открытого состава в плане разработки и адаптации новых юридически обязывающих стандартов, которые будут способствовать укреплению международной безопасности при использовании информационно-коммуникационных технологий.

Кроме того, необходимо, чтобы следующая рабочая группа открытого состава в период после 2025 года располагала возможностями для решения проблем, возникающих из-за значительного цифрового разрыва между странами-членами, который затрудняет разработку конкретных глобальных стратегий укрепления международной безопасности при использовании информационно-коммуникационных технологий.

Наконец, широкую поддержку получили неимоверные усилия председателя рабочей группы открытого состава, направленные на достижение консенсуса в работе этой группы, и Боливарианская Республика Венесуэла вновь подтверждает свое твердое намерение продолжать участвовать в этом процессе и поддерживать его.

Ответы, полученные от межправительственных организаций

Европейский союз

[Подлинный текст на английском языке]
[29 апреля 2024 года]

Киберпространство, в особенности глобальный открытый Интернет, стало одной из основ наших обществ. Оно служит платформой, обеспечивающей связь и экономический рост. Европейский союз и его государства-члены выступают за глобальное, открытое, стабильное, мирное и безопасное киберпространство, функционирующее при соблюдении верховенства права, прав человека, основных свобод и демократических ценностей, которые обеспечивают социальное, экономическое и политическое развитие во всем мире.

Международное сообщество признает, что действующие нормы международного права, в частности Устав Организации Объединенных Наций во всей его полноте, применимы к действиям государств в киберпространстве и существенно необходимы для поддержания мира и стабильности и развития открытой, безопасной, мирной и доступной среды ИКТ.

Консенсусные рекомендации Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2010, 2013, 2015 и 2021 годов, консенсусная рекомендация Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности 2021 года и консенсусные ежегодные доклады 2022 и 2023 годов о ходе работы, представленные рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, позволили разработать и консолидировать нормативные рамки ответственного поведения государств в киберпространстве. Эти нормативные рамки предусматривают применение международного права в киберпространстве, добровольные нормы ответственного поведения государств, меры укрепления доверия и наращивание потенциала.

Европейский союз и его государства-члены подтверждают свое твердое намерение действовать в соответствии с достигнутыми договоренностями и международным правом, включая Устав во всей его полноте, а также нормами ответственного поведения государств в киберпространстве. Мы твердо наме-

рены поощрять мир и стабильность в киберпространстве и добиваться прогресса в их укреплении посредством обсуждений и работы, в частности на таких форумах, как нынешняя рабочая группа открытого состава.

Исходя из этой позиции и нашей поддержки деятельности рабочей группы открытого состава Европейский союз не смог поддержать резолюцию [78/237](#) «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности», принятую Генеральной Ассамблеей 22 декабря 2023 года.

Европейский союз считает, что резолюция могла бы лучше отразить хрупкий консенсус, достигнутый в рабочей группе открытого состава, предшествующие процессы и предыдущие консенсусные резолюции.

Прежде всего, в резолюции не упоминаются суммарные и эволюционирующие нормативные рамки ответственного поведения государств при использовании ИКТ — рамки, которые являются результатом переговоров, идущих более 20 лет, и которые неоднократно были одобрены Генеральной Ассамблеей на основе консенсуса.

Вместо этого в ней, в частности в шестнадцатом пункте преамбулы и пункте 5 постановляющей части, содержатся отдельные предложения по вопросам существа, которые были поддержаны небольшой группой государств и которые, как опасается Европейский союз, могут препятствовать постепенному и основанному на консенсусе подходу, благодаря которому рабочей группе открытого состава удавалось добиваться прогресса на протяжении последних лет.

Европейский союз и его государства-члены считают, что имплементация принятых Организацией Объединенных Наций рамок ответственного поведения государств при использовании ИКТ имеет первостепенное значение для обеспечения открытой, безопасной, стабильной, доступной и мирной среды ИКТ, и мы обеспокоены тем, что эта резолюция основывается на формулировках, которые не были приняты консенсусом и которые могут привести к пересмотру результатов деятельности рабочей группы открытого состава и имеющихся консенсусных документов.

Европейский союз сохраняет полную приверженность поиску общей позиции для достижения консенсуса в рамках действующей рабочей группы открытого состава, а также приверженность коллективным усилиям, направленным на разработку инклюзивного, постоянного и ориентированного на действия механизма для регулярного институционального диалога, который будет проводиться после завершения работы действующей рабочей группы открытого состава.

Мнения, запрошенные в соответствии с пунктом 8 резолюции

Был достигнут значительный прогресс в обсуждении механизма, который начнет функционировать по завершении деятельности рабочей группы открытого состава 2021–2025 годов. В докладе Генерального секретаря ([A/78/76](#)), представленном во исполнение резолюции [77/37](#) Генеральной Ассамблеи, приводятся наблюдения и заключения относительно сферы охвата, структуры, принципов, содержания, подготовительной работы и форм учреждения программы действий по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности. Кроме того, рабочая группа открытого состава 2021–2025 годов в своем ежегодном докладе за 2023 год привела согласованные общие элементы будущего механизма для регулярного институционального диалога. Наконец, председатель рабочей группы открытого состава 2021–2025 го-

дов предложил дополнительные общие элементы в дискуссионном документе, составленном на основе предложений делегаций и обсуждений, состоявшихся на шестой основной сессии рабочей группы открытого состава.

Принимая во внимание прогресс, достигнутый в определении общих элементов для будущего механизма регулярного институционального диалога, Европейский союз продолжит излагать свои взгляды на этот механизм.

Укрепление международной безопасности и стабильности в киберпространстве, а также углубление понимания и имплементация нормативных рамок Организации Объединенных Наций по ответственному поведению государств в киберпространстве должны оставаться приоритетами регулярного институционального диалога по этим вопросам, проводимого под эгидой Организации Объединенных Наций.

В ответ на призыв к налаживанию постоянного, инклюзивного, транспарентного институционального диалога с широким участием под эгидой Организации Объединенных Наций, сформулированный в докладах 2021 года Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов, межрегиональная группа стран выдвинула предложение по программе действий, предусматривающее возможность создать постоянную структуру для регулярного институционального диалога на уровне Организации Объединенных Наций и тем самым позволить международному сообществу сосредоточить свои дискуссии на вопросах существа вместо того, чтобы вести постоянные споры о будущих процессах¹. Таким образом, программа может стать эволюционирующим механизмом для будущего сотрудничества в рамках Первого комитета Генеральной Ассамблеи.

Для этого коллективное внимание следует сосредоточить на поиске баланса между двумя одинаково важными аспектами нашей работы — имплементацией установленных рамок ответственного поведения государств при использовании ИКТ в контексте международной безопасности и дальнейшим развитием этих рамок. Развивать нормативные рамки предполагается, в частности, на основе уроков, извлеченных в ходе выполнения взятых обязательств.

Механизм должен быть инклюзивным, ориентированным на действия и служить площадкой для детальных обсуждений и обмена мнениями, способствовать наращиванию потенциала и обеспечивать дальнейшее развитие нормативных рамок и их обновление на основе консенсуса в соответствии с изменениями, происходящими в сфере ИКТ.

Он должен также предусматривать официальное участие соответствующих заинтересованных сторон, включая частный сектор, академические круги и гражданское общество, и регулярные консультации с ними, с тем чтобы они могли обсуждать соответствующие вопросы и излагать свои особые точки зрения и делиться знаниями. Это позволит еще активнее сосредоточиться на оказании государствам поддержки в содействии имплементации нормативных рамок ответственного поведения государств и на наращивании потенциала с учетом потребностей в целях повышения киберустойчивости как на национальном, так и на глобальном уровнях.

Программа действий должна основываться на нормативных рамках, содержащихся в последовательных консенсусных докладах Группы правительственных экспертов и рабочей группы открытого состава и вытекающих из них

¹ См. <https://documents.unoda.org/wp-content/uploads/2021/11/Working-paper-on-the-proposal-for-a-Cyber-PoA.pdf>.

обязательствах и действиях. Будущий механизм должен раз в несколько лет (например, каждые три-четыре года) созывать периодические обзорные конференции для рассмотрения и, при необходимости, обновления нормативных рамок ответственного поведения государств, а также для определения стратегического направления работы механизма.

Например, в рамках программы действий можно было бы проводить ежегодные официальные сессии, на которых будут обобщаться итоги открытых подробных обсуждений, созываемых в течение года. На ежегодных официальных сессиях можно было бы принимать решения об организации технических совещаний, рабочих групп или рабочих секций открытого состава, предназначенных для решения конкретных приоритетных задач программы действий.

Участие в технических рабочих секциях должно быть добровольным и открытым для всех государств. Решения об организации рабочих секций, в том числе об участии заинтересованных сторон, и периодичности заседаний, должны приниматься на ежегодных совещаниях или обзорных конференциях. Эти заседания должны быть ориентированы на разработку итогового документа, в котором в порядке постоянного совершенствования будут приводиться оперативные выводы из уроков, извлеченных в ходе имплементации рамок ответственного поведения государств.

Программа действий могла бы также расширить региональное участие путем привлечения к сотрудничеству региональных организаций, чтобы использовать их соответствующие инициативы и использовать имеющиеся структуры и платформы по наращиванию потенциала. Такие коллективные усилия будут способствовать определению странами своих потребностей в наращивании потенциала и получению необходимой помощи. Подчеркивая главную ответственность государств за поддержание международного мира и безопасности и их центральную роль в программе действий, мы в то же время считаем, что следует укрепить обмен мнениями и сотрудничество с заинтересованными сторонами, обеспечив площадку для инклюзивного и конструктивного участия.

Что касается подготовительной работы и учреждения программы действий, то в 2024 и 2025 годах следует организовать межсессионные совещания и специальные сессии рабочей группы открытого состава, чтобы продолжить проработку различных аспектов программы действий, включая бюджетные последствия создания постоянного механизма и определение в рамках Организации Объединенных Наций субъектов для выполнения соответствующих функций. Итоги этих совещаний должны отражаться в соответствующих ежегодных докладах рабочей группы открытого состава. Программа действий должна начать функционировать по завершении деятельности рабочей группы открытого состава 2021–2025 годов.