Организация Объединенных Наций A/AC.292/2024/2

Генеральная Ассамблея

Distr.: General
22 January 2024
Russian
Original: English

Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025
Седьмая основная сессия
Нью-Йорк, 4–8 марта 2024 года

Картирование с целью изучения ситуации с программами и инициативами по наращиванию потенциала в рамках Организации Объединенных Наций и за ее пределами, на глобальном и региональном уровнях

Документ Секретариата

I. Введение

1. В пункте 46 доклада о ходе обсуждения Рабочей группой пункта 5 повестки дня, который содержится в приложении к документу, озаглавленному «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности» (A/78/265), Секретариату Организации Объединенных Наций было предложено провести картирование процесса в консультации с соответствующими структурами с целью изучения ситуации с программами и инициативами по наращиванию потенциала в рамках Организации Объединенных Наций и за ее пределами, на глобальном и региональном уровнях, в том числе путем выяснения мнений государств-членов. Секретариату было предложено также подготовить доклад с результатами такого картирования и представить его на седьмой сессии Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, которая состоится 4–8 марта 2024 года, тем самым поддержав работу государств по оценке существующих усилий по наращиванию потенциала в области безопасности ИКТ и способствовать дальнейшему взаимоусилению и координации таких усилий. Настоящий доклад представляется во исполнение этой просьбы.

2. 2 октября 2023 года Управление по вопросам разоружения распространило вербальную ноту среди всех постоянных представительств при Организации Объединенных Наций, обратив их внимание на пункт 46 вышеупомянутого доклада и предложив им высказать свое мнение о ситуации с программами и инициативами по наращиванию потенциала в области информационно-коммуникационных технологий в Организации Объединенных Наций и за ее пределами, на

глобальном и региональном уровнях. Крайний срок представления ответов был установлен на 10 ноября 2023 года, а затем продлен до 16 ноября. По состоянию на 22 января 2024 года письменные мнения представили следующие государства: Австралия, Бельгия, Бразилия, Буркина-Фасо, Германия, Индия, Иран (Исламская Республика), Камбоджа, Катар, Колумбия, Куба, Ливан, Мексика, Нидерланды (Королевство), Португалия, Республика Корея, Российская Федерация, Сингапур, Словакия, Словения, Соединенное Королевство Великобритании и Северной Ирландии, Соединенные Штаты Америки, Турция, Уругвай, Франция, Чехия, Чили, Швейцария и Эстония.

3. Управление по вопросам разоружения также запросило мнения соответствующих подразделений системы Организации Объединенных Наций в письмах от 2 октября 2023 года. По состоянию на 22 января 2024 года письменные мнения представили следующие подразделения Организации Объединенных Наций: Международный союз электросвязи, Исполнительный директорат Контртеррористического комитета, Программа развития Организации Объединенных Наций, Институт Организации Объединенных Наций по исследованию проблем разоружения, Межрегиональный научно-исследовательский институт Организации Объединенных Наций по вопросам преступности и правосудия, Контртеррористическое управление, Управление информационно-коммуникационных технологий, Управление по правовым вопросам и Управление Организации Объединенных Наций по наркотикам и преступности.

4. Кроме того, 2 октября 2023 года соответствующим неправительственным заинтересованным организациям по электронной почте был разослан призыв представить свои материалы. По состоянию на 22 января 2024 года письменные мнения представили следующие заинтересованные стороны: Ассоциация за прогресс в области коммуникаций, Центр по регулированию коммуникаций при Национальном юридическом университете Дели, фонд «Дипло», Глобальный форум по обмену опытом в области компьютерных технологий, Международная торговая палата, Центр передового опыта по национальной безопасности Школы международных исследований имени С. Раджаратнама и организации «Сейф ПиСи солюшенз», «Тёрд ай лигал» и «Райт пайлот». Свое мнение представил также Европейский союз. Кроме того, были получены следующие совместные письменные материалы: совместное представление от Аргентины, Бразилии, Гватемалы, Доминиканской Республики, Колумбии, Коста-Рики, Парагвая, Сальвадора, Уругвая, Чили и Эквадора; и совместное представление Национального агентства кибербезопасности и информационной безопасности Чехии, Международного комитета Красного Креста (МККК), Центра передового опыта Организации Североатлантического договора (НАТО) по совместной киберзащите, Эксетерского университета, Военно-морского колледжа Соединенных Штатов и Уханьского университета.

5. Все полученные письменные мнения, включая те, которые были получены после официального продления срока, размещены на веб-сайте Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025[1]. Государствам рекомендуется ознакомиться с полным текстом письменных материалов, представленных государствами-членами, учреждениями системы Организации Объединенных Наций и неправительственными заинтересованными сторонами, поскольку в настоящем докладе упоминаются не все описанные в них мероприятия.

6. Настоящий доклад подготовлен преимущественно на основе материалов, полученных от перечисленных выше государств-членов, подразделений

[1] См. по ссылке https://meetings.unoda.org/meeting/57871/documents.

системы Организации Объединенных Наций и неправительственных заинтересованных структур, без ущерба для их индивидуальных позиций. Дополнительная информация, доступная из открытых источников, представлена с целью создания сбалансированной и наглядной картины существующих программ и инициатив по наращиванию потенциала в рамках Организации Объединенных Наций и за ее пределами, на глобальном и региональном уровнях.

7. Приводятся примеры программ и инициатив по наращиванию потенциала, причем сначала освещаются усилия на региональном и субрегиональном уровнях, а затем информация в целом классифицируется по темам. Эти описания не представляют собой исчерпывающий перечень всех инициатив и программ по наращиванию потенциала, а скорее направлены на то, чтобы дать общее представление о деятельности в иллюстративном порядке. Расстановки приоритетов или ранжирования мероприятий не предусмотрено.

8. В конце настоящего доклада приводятся замечания и выводы Секретариата, призванные помочь государствам в реализации более эффективных, устойчивых и действенных инициатив по наращиванию потенциала на глобальном, региональном и субрегиональном уровнях.

II. Обзор обсуждений и выводов государств по вопросам наращивания потенциала на многостороннем уровне

9. В свете постоянного изменения ситуации с угрозами, сопряженными с использованием государствами информационно-коммуникационных технологий в контексте международной безопасности, государства продолжают подчеркивать настоятельную необходимость укрепления потенциала всех государств по соблюдению и применению кумулятивных и эволюционирующих рамок ответственного поведения государств, как это подтверждается во втором ежегодном докладе Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 (A/78/265).

10. Государства подчеркнули необходимость способствовать лучшему пониманию потребностей развивающихся государств в целях сокращения цифрового разрыва посредством целенаправленных усилий по наращиванию потенциала. Государства подчеркнули острую необходимость наращивания потенциала и обмена передовым опытом по целому ряду дипломатических, правовых, политических, законодательных и нормативных направлений, в дополнение к развитию технических навыков, наращиванию институционного потенциала и работе механизмов сотрудничества. Государства не раз подчеркнули ценность сотрудничества Юг — Юг, трехстороннего, субрегионального и регионального сотрудничества, дополняющих сотрудничество Север — Юг. Кроме того, государства напомнили о ценности подхода, основанного на подготовке инструкторов, путем создания специализированных учебных программ и специализированных учебных планов, а также профессиональной сертификации, что позволит передавать необходимые знания и навыки соответствующим партнерам.

11. В рамках деятельности Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 государства продолжают вносить конкретные практико-ориентированные предложения в отношении усилий по наращиванию потенциала, включая, в частности, предложение о создании глобального портала сотрудничества в области кибербезопасности, предложение о поощрении дальнейшего технического обмена информацией об угрозах, связанных с информационно-коммуникационными технологиями, в целях выявления, обнаружения и содействия принятию обоснованных мер

реагирования на вредоносную деятельность, а также предложение о проведении обсуждений по вопросам содействия конструктивному взаимодействию и партнерству с неправительственными заинтересованными сторонами в области наращивания потенциала, в том числе для целей подготовки кадров и проведения исследований.

12. Сама Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 была признана платформой для дальнейшего обмена мнениями и идеями относительно усилий по наращиванию потенциала, в том числе относительно того, как лучше использовать существующие инициативы, чтобы поддержать государства в развитии институциональных возможностей применения рамок ответственного поведения государств.

13. Государства продолжают содействовать учету принципов наращивания потенциала в связи с использованием государствами информационно-коммуникационных технологий в контексте международной безопасности, которые содержатся в приложении C к документу A/78/265 и впервые были сформулированы в заключительном докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности[2]. Одобрив эти принципы, государства пришли к выводу, что процесс наращивания потенциала должен быть устойчивым, включать в себя конкретные ориентированные на результат мероприятия и иметь ясную цель, будучи при этом основанным на фактах, политически нейтральным, транспарентным, подотчетным и безоговорочным. Кроме того, государства согласились с тем, что наращивание потенциала должно осуществляться при полном признании принципа государственного суверенитета и соблюдении прав человека и основных свобод, определяться спросом и соответствовать определяемым государствами потребностям и приоритетам. В своем втором очередном докладе (A/78/265) Рабочая группа открытого состава рекомендовала государствам разработать и распространить добровольные контрольные перечни и другие инструменты для учета процесса осуществления согласованных принципов наращивания потенциала.

14. В рамках обсуждений в рамках Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 государства продолжали повышать осведомленность о гендерных аспектах безопасности при использовании информационно-коммуникационных технологий и содействовать наращиванию потенциала с учетом гендерных факторов на уровне политики, а также при отборе и реализации проектов по наращиванию потенциала. Государства поощряли усилия по содействию наращиванию потенциала с учетом гендерных аспектов, в том числе путем интеграции гендерных аспектов в политику и инициативы по наращиванию потенциала в области информационно-коммуникационных технологий на национальном уровне, а также разработки контрольных перечней или вопросников для выявления потребностей и пробелов в этой области.

15. Государства считают, что Организация Объединенных Наций могла бы играть важную роль в координации усилий по наращиванию потенциала, оценивая потребности государств, выявляя пробелы с помощью инструментов и обследований и облегчая доступ государств к программам наращивания потенциала, в том числе в рамках нынешнего картирования.

[2] A/75/816, приложение I, п. 56.

III. Региональное, субрегиональное и межрегиональное сотрудничество

16. Государства неизменно подтверждают, что региональные и субрегиональные организации играют важную роль в содействии реализации рамок ответственного поведения государств при использовании информационно-коммуникационных технологий, в том числе в формате поддержки соответствующих инициатив по наращиванию потенциала. Государства по-разному оценивали усилия, которые можно было бы предпринять на региональном, субрегиональном и межрегиональном уровнях, включая семинары, учебные курсы и обмен передовым опытом и извлеченными уроками. Кроме того, государствам было рекомендовано поддерживать программы по наращиванию потенциала, в том числе, в соответствующих случаях, в сотрудничестве с региональными и субрегиональными организациями[3].

17. Что касается межрегионального сотрудничества, то Глобальный форум по обмену опытом в области компьютерных технологий — это многостороннее сообщество, включающее более 200 членов и партнеров, в том числе государства из всех регионов, международные и региональные организации, а также представителей частного сектора, гражданского общества и научных кругов. Портал “Cybil”, ведущая инициатива Глобального форума по обмену опытом в области компьютерных технологий, представляет собой онлайн-хранилище международных проектов по наращиванию потенциала в области кибербезопасности и содержит библиотеку ресурсов для заинтересованных сторон[4].

18. В ноябре 2023 года Глобальный форум по обмену опытом в области компьютерных технологий в сотрудничестве с Ганой, Всемирным экономическим форумом, Всемирным банком и Институтом кибермира провел первую Глобальную конференцию по наращиванию потенциала в области кибербезопасности. В рамках конференции состоялись тематические и углубленные региональные занятия. На конференции был принят итоговый документ — Аккрский призыв к противодействию киберугрозам в контексте развития, включающий ряд необязательных, добровольных, задающих направление деятельности мероприятий, которые направлены на: a) повышение роли потенциала противодействия киберугрозам как фактора, способствующего устойчивому развитию; b) содействие наращиванию обусловленного спросом, эффективного и устойчивого потенциала в области кибербезопасности; c) содействие укреплению партнерских связей и улучшению координации; и d) получение доступа к финансовым ресурсам и механизмам реализации[5]. На конференции было объявлено, что следующая глобальная конференция по наращиванию потенциала в области кибербезопасности, призванная развить успехи, достигнутые в Гане, пройдет в Женеве в мае 2025 года.

19. В целях укрепления сотрудничества между регионами Цифровой альянс Европейского союза — Латинской Америки и Карибского бассейна проводит диалоги по вопросам регулирования и кибербезопасности, а также другие мероприятия по цифровой и космической тематике. Альянс стремится поддерживать цифровые преобразования и инновации, ориентируясь на нужды людей в контексте цифровых экономик и обществ. Для достижения этих целей Деятельность Альянса включает: создание межрегионального диалога по цифровой политике,

[3] A/78/265, приложение, п. 51.

[4] См. https://cybilportal.org/about-cybil/.

[5] Доступно на сайте https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development/.

расширение программы «Создание европейской связи с Латинской Америкой», реализация региональной стратегии «Коперник» для повышения цифровой устойчивости к потрясениям путем укрепления потенциала управления пространственными данными и поддержки их стратегического использования, а также создание регионального цифрового акселератора Европейского союза — Латинской Америки и Карибского бассейна для содействия развитию предпринимательства и инноваций.

20. Текущий проект под названием «Укрепление сотрудничества в области безопасности в Азии и с Азией», поддерживаемый Европейским союзом и финансируемый Францией и Германией, направлен на сближение политики и практики Европейского союза и стран-партнеров, повышение осведомленности и поддержку оперативных диалогов по вопросам безопасности[6]. В рамках этого проекта проводятся мероприятия по четырем тематическим направлениям: борьба с терроризмом и предотвращение насильственного экстремизма, кибербезопасность, безопасность на море и кризисное управление. В настоящее время его государствами-участниками являются Вьетнам, Индия, Индонезия, Республика Корея, Сингапур и Япония.

21. В регионе Центральной и Восточной Европы в мае 2023 года Франция, Черногория и Словения создали Центр потенциала в области кибербезопасности Западных Балкан[7]. Центр призван оказать поддержку шести участвующим странам и областям в укреплении потенциала в области кибербезопасности на институциональном и оперативном уровнях. Его деятельность включает в себя проведение учебных курсов, разработку учебных программ по кибертехнологиям и обмен информацией и передовым опытом для поддержки специалистов-практиков в западнобалканских государствах в предотвращении киберугроз, подготовке к ним и реагировании на них. В 2023 году Центр провел учебные курсы по кибергигиене для государственных административных органов, организовал программу наставничества для женщин в области киберполитики и международных переговоров, провел занятия по киберпреступности для работников судебных органов и полиции и организовал курс занятий для руководителей служб информационной безопасности объектов критически важной инфраструктуры. На момент подготовки настоящего документа еще 12 учебных курсов запланированы на 2024 год. Аналогичным образом, проект Европейского союза под совместным руководством Чехии и Эстонии направлен на поддержку наращивания потенциала кибербезопасности на Западных Балканах путем развития следующих направлений: a) регулирование кибербезопасности и повышение осведомленности; b) укрепление правовых рамок, кибернорм и соблюдения норм международного права; c) управление рисками и кризисное управление; и d) укрепление оперативного потенциала, в том числе путем усиления группы реагирования на инциденты в сфере компьютерной безопасности. Еще один проект Европейского союза под названием «Быстрое реагирование в области кибербезопасности для Албании, Черногории и Северной Македонии» был реализован для поддержки потенциала противодействия киберинцидентам.

22. Департамент транснациональных угроз Организации по безопасности и сотрудничеству в Европе (ОБСЕ) осуществляет деятельность, направленную на укрепление потенциала государств-участников в борьбе с угрозами в сфере информационно-коммуникационной безопасности. В число проводимых мероприятий входят практические занятия в поддержку надлежащего государственного реагирования на инциденты, затрагивающие объекты критически важной инфраструктуры, семинары по противодействию использованию Интернета в тер-

[6] См. https://www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf.
[7] См. https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c/.

ристических целях и занятия по расследованию киберпреступлений и соответствующему судебному преследованию[8]. В 2023 году Департамент организовал в Вене учебный курс по международной кибердипломатии, направленный на укрепление национального потенциала для участия в дискуссии о киберполитике на международном уровне. ОБСЕ, выступая в качестве механизма внедрения национальных шкал оценки тяжести киберинцидентов и соответствующих мер по защите объектов критически важной инфраструктуры, поддерживает разработку процедур кризисной коммуникации и управления, а также методов классификации инцидентов среди стран Европы, Центральной Азии и других регионов. Кроме того, ОБСЕ служит многосторонним форумом для проведения ряда дискуссий по вопросам сотрудничества и наращивания потенциала в сфере кибербезопасности.

23. Российская Федерация проводит в сотрудничестве с Региональным форумом Ассоциации государств Юго-Восточной Азии (АСЕАН) ежегодные семинары и онлайн-практикумы по терминологии в области безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, противодействия использованию информационно-коммуникационных технологий в преступных целях, устойчивого и безопасного развития Интернета и цифровой криминалистики. Кроме того, Российская Федерация организовала — в рамках Совещания по взаимодействию и мерам доверия в Азии — занятия по расследованию преступлений, связанных с хищениями в сфере информационно-коммуникационных технологий.

24. Международный союз электросвязи (МСЭ) в сотрудничестве с Международным многосторонним партнерством по борьбе с киберугрозами при поддержке Омана создал Региональный центр кибербезопасности Омана и МСЭ[9]. Центр, базирующийся в помещениях группы реагирования на компьютерные инциденты Омана, призван повысить потенциал, возможности, готовность, навыки и знания в области кибербезопасности, защиты объектов критически важной инфраструктуры и наращивания потенциала для арабского региона.

25. В рамках своей Программы по кибербезопасности Межамериканский комитет по борьбе с терроризмом Организации американских государств (ОАГ) оказывает поддержку государствам-членам в наращивании технического, политического и дипломатического потенциала для предотвращения и выявления киберинцидентов, реагирования на них и преодоления их последствий, а также для поощрения ответственного поведения государств в киберпространстве[10]. Направления деятельности Программы включают, среди прочего, оказание помощи в разработке национальных стратегий кибербезопасности и создание национальных групп реагирования на инциденты в сфере компьютерной безопасности. Кроме того, в рамках этой программы оказывается помощь и проводится обучение, предоставляются методические пособия и руководства для политиков, представителей промышленности и гражданского общества, а также поддерживается работа сети групп реагирования на инциденты в сфере компьютерной безопасности полушария Северной и Южной Америки, которая делится информацией об угрозах и оперативными данными с 29 группами реагирования на инциденты в сфере компьютерной безопасности из 20 государств — членов ОАГ. Кроме того, эта программа способствует более полному учету гендерных аспектов при разработке политики в области кибербезопасности и обеспечению представленности в многосторонних процессах.

[8] См. https://www.osce.org/secretariat/cyber-ict-security.

[9] См. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.spx.

[10] См. https://www.oas.org/ext/en/security/prog-cyber.

26. В октябре 2023 года в Бразилии состоялся Иберо-американский форум по киберзащите[11]. В работе форума, целью которого было углубление региональной интеграции и сотрудничества в области предотвращения, выявления и устранения киберугроз, приняли участие 13 государств. Мероприятия включали в себя имитационные учения и тренировки, в том числе учения “Cyber Guardian 5.0” и разработку платформы для обмена информацией о вредоносных программах.

IV. Неполный иллюстративный обзор инициатив по наращиванию потенциала по тематическим направлениям

Международное право

27. Государства признали особую необходимость в инициативах по наращиванию потенциала в области международного права в контексте информационно-коммуникационной безопасности. Государства подчеркнули настоятельную необходимость продолжения такой работы по наращиванию потенциала, в том числе с целью обеспечения возможностей для всех государств на равных участвовать в выработке общего понимания того, как международное право применяется к использованию информационно-коммуникационных технологий. Эти усилия включали проведение семинаров, учебных курсов и обменов передовым опытом на международном, межрегиональном, региональном и субрегиональном уровнях. Кроме того, государства отметили ценность наращивания потенциала с целью подготовки национальных документов с изложением позиции по вопросу о применимости норм международного права к использованию государствами информационно-коммуникационных технологий.

28. Имеющиеся на глобальном уровне онлайн-ресурсы, посвященные наращиванию потенциала в области международного права, включают Инструментарий по киберправу, разработанный консорциумом в составе Национального агентства кибербезопасности и информационной безопасности Чехии, МККК, Центра передового опыта НАТО по совместной киберзащите, Эксетерского университета, Военно-морского колледжа США и Уханьского университета[12]. Этот инструментарий имеется в бесплатном доступе для государственных органов и специалистов в области права и в настоящее время содержит: a) 28 сценариев, в которых рассматривается применимость международного права к кибероперациям; b) информацию о национальных позициях по вопросу о применимости норм международного права к использованию информационно-коммуникационных технологий, в том числе в том, что касается суверенитета, невмешательства или того, что считается нападением в соответствии с нормами международного гуманитарного права; и c) более 50 страниц, посвященных киберинцидентам, на которых представлена информация о недавних нападениях или текущих вооруженных конфликтах.

29. Оксфордский процесс по международно-правовой защите в киберпространстве был начат в 2020 году Оксфордским институтом этики, права и вооруженных конфликтов в партнерстве с компанией «Майкрософт»[13]. На момент подготовки настоящего документа в рамках Оксфордского процесса было подготовлено пять «Оксфордских заявлений о международно-правовой защите», которые являются результатом сотрудничества международных экспертов в области права по всему миру с целью определения и разъяснения норм междуна-

[11] См. https://dialogo-americas.com/articles/brazil-leads-ibero-american-cyber-defense-forum/.
[12] См. https://cyberlaw.ccdcoe.org/wiki/Main_Page.
[13] См. https://www.elac.ox.ac.uk/the-oxford-process/.

родного права, применимых к кибероперациям в различных контекстах, включая защиту сектора здравоохранения, охрану исследований вакцин, защиту от вмешательства в выборы, регулирование информационных операций и деятельности, а также операций с вирусами-вымогателями.

30. Что касается применимости международного гуманитарного права к киберпространству, МККК предоставляет ресурсы для политиков, в том числе исследовательские работы, семинары, симпозиумы и создание делегации МККК по киберпространству, базирующейся в Люксембурге и пользующейся его поддержкой. Примеры недавних мероприятий включают запуск программы гуманитарной деятельности в сотрудничестве с Центром исследований в области искусства, социальных и гуманитарных наук Кембриджского университета, проведение, совместно с Женевской академией международного гуманитарного права и прав человека, международного совещания экспертов по международному гуманитарному праву и растущему участию гражданского населения в кибероперациях и других цифровых операциях во время вооруженных конфликтов, которое состоялось 28–29 сентября 2023 года в Женеве, а также организация, в партнерстве с Исследовательским обществом международного права, круглого стола по кибервойнам, который прошел 17 мая 2023 года в Исламабаде.

31. Австралия, Нидерланды (Королевство) и Сингапур совместно с международной компанией «Киберправо» координируют проведение международного учебного курса в сфере киберправа для государственных служащих государств — членов АСЕАН и ОБСЕ по международному праву кибероперациий.

32. В рамках занятий по наращиванию потенциала в области международного права и формирования политики для усиления мер по обеспечению кибербезопасности Японское агентство международного сотрудничества предоставляет должностным лицам государственных учреждений и национальных групп реагирования на компьютерные инциденты из развивающихся стран знания и навыки в области международного права и политики, необходимые им для эффективной разработки и реализации политики кибербезопасности.

33. Кроме того, государства проводят различные консультации, чтобы создать условия для диалога о применимости международного права. Так, ОАГ провела в сотрудничестве с Межамериканским юридическим комитетом и МККК консультации по нормам международного права, применимым к киберпространству[14]. Кроме того, Мексика провела в сотрудничестве с Институтом права, инноваций и технологий Темпльского университета Пенсильвании и компанией «Майкрософт» три виртуальных семинара по применению норм международного права в киберпространстве, поощрению правил и норм мирного поведения и преодолению цифрового разрыва. В рамках проекта был подготовлен многосторонний сборник примеров передовой практики и рекомендаций по применению международного права в киберпространстве, который был представлен в декабре 2023 года на шестой основной сессии Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ.

34. ОБСЕ организовала исполнительные курсы по международному праву кибероперациий, включая курс, который пройдет с 13 по 17 февраля 2023 года в Скопье в сотрудничестве с Королевством Нидерландов при дополнительной поддержке Италии, Словакии, Швейцарии, Соединенного Королевства Великобритании и Северной Ирландии и Республики Корея, а также международной компании «Киберправо».

[14] См. https://www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp.

Политика, включая разработку национальных стратегий

35. В приложении B к своему второму годовому докладу о ходе работы, содержащемуся в документе A/78/265, Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025 согласовала первоначальный перечень добровольных глобальных мер укрепления доверия. В рамках одной из этих мер государствам рекомендуется продолжать на добровольной основе обмен информацией о концептуальных документах, национальных стратегиях, директивных мерах и программах. Кроме того, государства признают важность наличия необходимого потенциала для разработки требуемых директивных мер, законодательных актов и стратегий для создания безопасной информационно-коммуникационной среды. В этих условиях были предприняты различные усилия по наращиванию потенциала, призванные помочь государствам сформулировать национальную политику, разработать стратегии и создать необходимые институты и структуры соответствующего профиля в сфере информационно-коммуникационных технологий в контексте международной безопасности.

36. Что касается глобального уровня, Институт Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР) проводит ежегодную конференцию по стабильности в киберпространстве, на которой обсуждаются вопросы обеспечения безопасного и стабильного киберпространства, норм и международного права, а также поддержки многостороннего диалога по вопросам кибербезопасности. В прошлые годы в рамках конференции проводились тематические брифинги ученых, призванные содействовать выработке национальных позиций государств, в том числе по правовым вопросам, связанным с мирным урегулированием споров в связи с использованием государствами информационно-коммуникационных технологий, а также по политическим и техническим вопросам защиты объектов критически важной инфраструктуры и жизненно важных услуг в различных секторах. На прошлых конференциях также уделялось внимание соответствующим межправительственным процессам под эгидой Организации Объединенных Наций. Следующая конференция по стабильности в киберпространстве состоится 29 февраля — 1 марта 2024 года в Нью-Йорке.

37. Государства также признали ценность портала по киберполитике ЮНИДИР, который обеспечивает государствам удобный формат для добровольного участия в мерах по обеспечению транспарентности путем обмена соответствующей информацией, в том числе о директивных и законодательных мерах и других примерах передовой практики[15]. По состоянию на декабрь 2023 года в базу данных портала по киберполитике было загружено 1528 документов; эти документы, опубликованные на 55 языках, содержат информацию о 897 проектах по наращиванию потенциала. В 2023 году портал насчитывал около 23 000 посещений.

38. В декабре 2023 года на портале по киберполитике была размещена информация о почти 900 проектах по наращиванию потенциала с портала “Cybil” Глобального форума по обмену опытом в области компьютерных технологий. Полученные данные, имеющиеся на шести официальных языках Организации Объединенных Наций, включают в себя сведения о проектах, в том числе названия проектов и информацию о бенефициарах, источниках финансирования и датах начала и окончания проектов. Эта инициатива способствует повышению безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий путем повышения осведомленности о существующих ресурсах, облегчения сотрудничества между

[15] См. https://cyberpolicyportal.org/.

заинтересованными сторонами и поощрения большей транспарентности в деле наращивания потенциала в области кибербезопасности.

39. МСЭ в партнерстве со Всемирным банком, Конференцией Организации Объединенных Наций по торговле и развитию (ЮНКТАД) и Организацией электросвязи стран Содружества оказывает политическую поддержку в создании эффективной национальной системы кибербезопасности. С этой целью во втором издании «Руководства по разработке национальной стратегии кибербезопасности», опубликованном МСЭ в 2021 году[16], вниманию принимающих решения лиц представлен обзор процесса разработки стратегии с учетом конкретной ситуации и культурных и общественных ценностей их страны. Кроме того, МСЭ разработал на основе Руководства учебный онлайн-курс для подготовки национальных политиков и специалистов-практиков в области кибербезопасности из государственного и частного секторов в формате четырех модулей электронного обучения и тренировочного онлайн-занятия[17]. Кроме того, в Интернете размещено обновленное хранилище информации о национальных стратегиях кибербезопасности, содержащее национальную политику, планы действий и другие соответствующие элементы, связанные с кибербезопасностью[18].

40. Стипендиальная программа Организации Объединенных Наций и Сингапура по кибербезопасности проводится дважды в год в формате шестидневной сессии для отобранных государственных чиновников с целью укрепления потенциала и сетей по вопросам национальных политических, стратегических и оперативных мер в области кибербезопасности и цифровой безопасности Первые три сессии в рамках этой программы уже состоялись, и еще две сессии запланированы на 2024 год. Сеть выпускников программы насчитывает более 70 стипендиатов из 62 государств-членов.

41. Королевство Нидерландов финансировало серию диалогов по глобальной киберполитике, которые проводились совместно с американским отделением Наблюдательного исследовательского фонда. В течение двух лет в рамках этого проекта осуществлялось содействие разработке национальных стратегий кибербезопасности и проводились региональные диалоги по киберполитике в странах Юго-Восточной Азии, Западных Балкан, Ближнего Востока и Северной Африки, Южной Африки и Латинской Америки и Карибского бассейна. Этот проект также был направлен на содействие безопасной цифровой трансформации и партнерству между государственным и частным секторами, выявление потребностей и пробелов в наращивании потенциала и поддержку дальнейшей разработки норм поведения государств в киберпространстве.

42. Европейский союз, Германия, организация «Экспертиза — Франция», Международный и иберо-американский фонд по вопросам администрации и государственного управления и Инициатива Африканского Рога объединили усилия в рамках деятельности Центра использования цифровых технологий в интересах развития для реализации инициативы по созданию цифрового правительства и обеспечению кибербезопасности в регионе Африканского Рога[19]. Цель этого проекта — помочь государствам-участникам (Джибути, Кения и Сомали) укрепить предоставление услуг государственного сектора через защищенные цифровые каналы. Проект включает в себя ведение диалогов и обмен

[16] См. https://ncsguide.org/the-guide/.
[17] См. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.
[18] См. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.
[19] См. https://www.fiiapp.org/en/proyectos_fiiapp/d4d-initiative-for-digital-governance-and-cybersecurity-idgc-for-the-horn-of-africa-initiative/.

информацией через региональный технический комитет, а также обзоры дорожных карт и проектов по оцифровке, реализуемых в каждом из государств.

43. На двусторонней основе Франция и Сенегал сотрудничают в рамках базирующейся в Дакаре национальной школы кибербезопасности региональной направленности, которая, помимо прочего, обеспечивает обучение, укрепляет сотрудничество и повышает осведомленность о кибербезопасности в африканских государствах[20]. В качестве наглядного примера еще одной из множества имеющихся двусторонних программ можно привести поддержку Португалией непрерывных программ стратегического сотрудничества в партнерстве с Анголой, Гвинеей-Бисау, Кабо-Верде, Мозамбиком, Сан-Томе и Принсипи и Тимором-Лешти, которые укрепляют правовые и административные структуры для предотвращения, выявления и пресечения киберпреступлений, кибертерроризма и киберинцидентов.

44. В Азии Глобальный центр кибербезопасности в целях развития, расположенный в Республике Корея, оказывает государствам по их просьбе помощь в развитии навыков в области кибертехнологий и потенциала противодействия киберугрозам в государственном секторе. Имеется возможность проводить семинары по разработке национальных стратегий и систем обеспечения кибербезопасности, созданию и функционированию национальных групп реагирования на компьютерные инциденты, обнаружению, анализу и пресечению киберинцидентов, а также обмену информацией о тенденциях и угрозах в киберпространстве[21]. Недавно в Коста-Рике, Лаосской Народно-Демократической Республике и Сербии были проведены семинары, посвященные, среди прочего, разработке стратегии кибербезопасности, обработке инцидентов, безопасному использованию киберпространства и потенциалу противодействия.

45. В рамках своей Программы сотрудничества в области кибертехнологий и важнейших технологий Министерство иностранных дел и торговли Австралии оказывает поддержку своему комиссару по электронной безопасности в разработке глобальных онлайн-ресурсов по безопасности и помощи правительствам стран Азии и Тихоокеанского региона в разработке национальных подходов к защите граждан в Интернете[22]. В рамках программы, осуществляемой в партнерстве с промышленными предприятиями, научными кругами, гражданским обществом, учреждениями правительства Австралии и другими донорами из числа единомышленников, оказывается поддержка более чем 25 странам Юго-Восточной Азии и Тихоокеанского региона в продвижении и защите их коллективных интересов в киберпространстве.

46. Что касается Северной и Южной Америки, то в январе 2023 года в рамках саммита лидеров стран Северной Америки Канада, Мексика и Соединенные Штаты Америки приняли участие в круглом столе по кибербезопасности с целью укрепления сотрудничества между государствами-участниками в разработке и осуществлении политики кибербезопасности. 8–14 октября 2023 года состоялись дискуссии по вопросам взаимопроникновения тем кибербезопасности и искусственного интеллекта с упором на законодательство, национальную политику и стратегии, совместно организованные Колумбией и Чехией.

47. Инициатива Европейского союза по кибердипломатии («Кибер-директ») направлена на содействие широкому спектру мер по директивной поддержке, проведению исследований, информационно-просветительской деятельности и

[20] См. https://www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal.

[21] См. https://www.kisa.or.kr/EN/201.

[22] См. https://www.internationalcybertech.gov.au/cyber-tech-cooperation-program.

наращиванию потенциала в области кибердипломатии, в том числе путем использования инструментария по кибердипломатии и проведения ежегодного Европейского диалога по кибердипломатии[23]. Помимо многих других программ и инициатив, «Кибер-директ» организует программу стипендий для специалистов младшего и среднего звена в области кибернетики и цифровых технологий из стран-партнеров, в частности, из не являющихся членами Европейского союза стран из Группы восточноевропейских государств, Группы африканских государств, Группы латиноамериканских и карибских государств и Группы азиатско-тихоокеанских государств[24]. Также в этом регионе коалиция Германии, Люксембурга Финляндии и Эстонии под руководством Управления информационных систем Эстонии занимается управлением и реализацией инициативы «Кибер-Сеть» Европейского союза на 2019–2025 годы[25], в рамках которой для поддержки развития потенциала в области кибербезопасности было создано сообщество из более чем 300 киберэкспертов по более чем 40 тематическим направлениям.

48. Женевский центр по управлению сектором безопасности осуществляет программу регулирования кибербезопасности, которая оказывает поддержку государственным субъектам по линии законодательных и директивных мер в области кибербезопасности в целях укрепления механизмов подотчетности и наращивании потенциала[26]. В рамках одного из недавних проектов была создана Западнобалканская исследовательская сеть кибербезопасности, которая, помимо прочего, проводит исследования в соответствующих национальных контекстах, касающиеся кибербезопасности и прав человека, потребностей уязвимых групп в плане кибербезопасности и гендерных аспектов. Аналогичным образом, Женевский центр по вопросам политики в области безопасности проводит учебные курсы и семинары по кибербезопасности[27]. Фонд «Дипло», который тоже расположен в Женеве, поддерживает развитие потенциала в области регулирования Интернета и цифровой политики, организуя онлайновые курсы, семинары и имитационные учения по кибербезопасности, данным, искусственному интеллекту и другим новым темам, а также поощряя использование цифровых инструментов для инклюзивного и эффективного управления и формирования политики и разрабатывая такие инструменты[28].

49. Проект «Киберпространство для всех», осуществляемый при поддержке Королевства Нидерландов, направлен на содействие инклюзивности и осведомленности путем создания единых формулировок и справочных материалов по международному киберуправлению, повышения осведомленности о ключевых событиях в области киберпространства в Организации Объединенных Наций и содействия в разработке государственной политики в области кибернорм. На первом этапе проект выпустил один номер журнала «Киберполитика», короткие видеоролики о наращивании потенциала в области кибербезопасности и подкаст «Кто правит киберпространством?». Второй этап, осуществляемый совместно с Чатем-Хаус, направлен на предоставление рекомендаций, повышение осведомленности и поддержку реализации норм и принципов Организации Объединенных Наций по наращиванию потенциала и ответственному поведению государств в киберпространстве.

[23] См. https://www.emspproject.eu/.
[24] См. https://eucyberdirect.eu/news/eu-cd-fellowship.
[25] См. https://www.eucybernet.eu/.
[26] См. https://www.dcaf.ch/cybersecurity-governance.
[27] См. https://www.gcsp.ch/.
[28] См. https://www.diplomacy.edu/.

50. Услуги по наращиванию потенциала в области кибердипломатии предлагаются по различным каналам. Так, в рамках программы «Многосторонность и цифровизация» при сотрудничестве Министерства иностранных дел Эстонии, Академии электронного управления и Эстонского центра международного развития организована Таллиннская летняя школа кибердипломатии. Ее основная цель — обучение дипломатов, занимающихся разработкой внешней киберполитики, а также других государственных служащих, интересующихся сложными вопросами, касающимися киберпространства. Кроме того, Программа кибербезопасности Межамериканского комитета по борьбе с терроризмом ОАГ проводит учебную программу по кибердипломатии для поддержки должностных лиц, работающих в этой области. Что касается Секретариата Организации Объединенных Наций, то в 2024 году будет обновлен онлайн-курс по кибердипломатии, который в настоящее время доступен на платформе «Информационная панель образования по вопросам разоружения»[29].

Группы реагирования на компьютерные инциденты, техническое обучение и другая соответствующая поддержка

51. Государства постоянно призывают применять конкретный и практико-ориентированный подход к наращиванию потенциала. Государства пришли к выводу, что такие конкретные меры могут включать оказание поддержки группам реагирования на компьютерные инциденты или группам реагирования на инциденты в сфере компьютерной безопасности, а также разработку специализированных программ обучения и специальных учебных планов, включая программы подготовки инструкторов и профессиональную сертификацию. Кроме того, государства выразили обеспокоенность тем, что недостаточная информированность о существующих и потенциальных угрозах и отсутствие надлежащих возможностей для выявления злонамеренных действий с использованием информационно-коммуникационных технологий, а также соответствующей защиты и реагирования могут сделать их более уязвимыми.

52. Была также отмечена важность технической подготовки кадров в сфере информационно-коммуникационных технологий, в том числе в области информационной безопасности, методов обнаружения и пресечения сетевых атак в открытых информационных системах, тактики, техники и процедур защиты информации от несанкционированного доступа, сбора данных из открытых источников, методов расследования преступлений, связанных с информационно-коммуникационными технологиями, в отношении международного мира и безопасности и международного сотрудничества в этой области, компьютерной криминалистики, противодействия использованию информационно-коммуникационных технологий и международных почтовых служб для незаконного оборота наркотиков и хищения средств, выявления и расследования незаконных операций с цифровыми активами, включая криптовалюты, и их использования для финансирования терроризма.

53. На глобальном уровне МСЭ оказывает постоянную помощь государствам в создании национальных групп реагирования на компьютерные инциденты[30]. Среди последних примеров — создание таких групп при содействии МСЭ на Багамских Островах, в Барбадосе, Буркина-Фасо, Гамбии, Гане, Замбии, Кении, Кипре, Кот-д'Ивуаре, Кыргызстане, Ливане, Малави, Объединенной Республике Танзания, Тринидаде и Тобаго, Уганде, Черногории и на Ямайке. В каждом

[29] См. https://cyberdiplomacy.disarmamenteducation.org/home/.
[30] См. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx.

случае эти группы служат центральным координирующим органом для выявления, обработки и пресечения киберугроз.

54. Форум групп оперативного реагирования и обеспечения безопасности поддерживает сеть из более чем 700 участвующих в ней групп реагирования на компьютерные инциденты для поддержки сотрудничества в целях профилактики инцидентов в сфере кибербезопасности и реагирования на них. Среди прочего Форум организует обмен передовым опытом между своими членами и способствует развитию технических коллоквиумов, занятий, публикаций, веб-услуг, групп по особым интересам и ежегодной конференции по реагированию на инциденты[31].

55. Секретарь Министерства электроники и информационных технологий Индии Алкеш Кумар Шарма торжественно открыл учения по кибербезопасности Группы двадцати, в которых приняли участие более 400 участников из этой страны и зарубежных участников в рамках председательства Индии в Группе двадцати. Индийская группа реагирования на компьютерные инциденты провела учения и тренировки по кибербезопасности в смешанном формате. Международные участники из 12 стран мира принимали участие онлайн. Представители таких отраслей Индии, как финансы, образование, телекоммуникации, порты и судоходство, энергетика и информационно-коммуникационные технологии приняли участие как очном, так и в виртуальном формате.

56. Соединенное Королевство, в период своего действующего председательства в Содружестве, провело ряд мероприятий по наращиванию потенциала в рамках Программы кибербезопасности Содружества в поддержку целей Кибердекларации Содружества 2018 года[32]. Программа оказывала поддержку государствам — членам Содружества в проведении самооценки национального потенциала в области кибербезопасности и предоставляла техническую помощь, обучение и консультации по вопросам кибербезопасности и угроз киберпреступности. В рамках проекта было проведено более 140 мероприятий в 32 странах, в которых приняли участие более 6000 человек.

57. Центр передового опыта в области кибербезопасности АСЕАН — Сингапур оказывает поддержку государствам — членам АСЕАН в наращивании потенциала в области кибербезопасности в регионе путем проведения исследований, обучения, оказания технической поддержки группам реагирования на компьютерные инциденты, обмена информацией о киберугрозах, атаках и примерах передового опыта из открытых источников, а также проведения практических занятий и учений[33]. С момента своего создания Центр передового опыта провел более 50 программ, в которых приняли участие более 1600 старших должностных лиц государств-участников. С 2024 года доступ к программам Центра передового опыта будет открыт и для государств, не входящих в регион АСЕАН. В целях поддержки регулярной координации и сотрудничества с 2016 года регулярно проводятся заседания Рабочей группы экспертов по кибербезопасности Расширенного совещания министров обороны стран-членов АСЕАН, выступающей в качестве платформы для укрепления доверия между государствами-членами АСЕАН и совместной разработки соответствующих норм.

58. Программа укрепления потенциала в области кибербезопасности АСЕАН направлена на наращивание потенциала государств-членов АСЕАН путем

[31] См. https://www.first.org/ .

[32] См. https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.

[33] См. https://www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.

укрепления устойчивости к потрясениям и усиления регионального реагирования на угрозы[34]. Среди мероприятий — мастер-классы, семинары, ежегодная Сингапурская международная кибернеделя, совместный американо-сингапурский семинар по кибербезопасности и конференция АСЕАН по кибербезопасности на уровне министров. В 2023 году в ходе восьмой Сингапурской международной кибернедели было начато осуществление Сингапурской программы лидеров и выпускников в области кибербезопасности. В рамках этой программы, открытой для кандидатов из всех государств, должностные лица проходят базовый, исполнительный и продвинутый курсы, позволяющие углубить их знания в области концепций и процессов кибердипломатии, международного права, норм в киберпространстве, а также оперативных и технических аспектов международной киберполитики. Кроме того, предполагается создать «Сообщество выпускников программы лидеров в области кибербезопасности», которое объединит бывших участников мероприятий по наращиванию потенциала, проводимых Центром передового опыта в области кибербезопасности, для проведения серии закрытых встреч, посвященных тенденциям, международному обсуждению вопросов кибербезопасности, а также для обмена передовым опытом в таких областях, как развитие трудовых ресурсов и навыков, правовые рамки и ответственное киберповедение.

59. Республика Корея выступает в качестве принимающей стороны Альянса по кибербезопасности в интересах взаимного прогресса с момента его создания в 2016 году. Деятельность Альянса направлена на развитие сотрудничества и наращивание потенциала между государствами-участниками[35]. На момент подготовки настоящего документа к Альянсу присоединились 67 организаций из 49 стран.

60. В 2023 году Корейское управление по Интернету и безопасности, в сотрудничестве с Канвонским национальным университетом, Университетом Каннын-Вонджу и Технологическим университетом Брунея, начало осуществление проекта «Киберщит АСЕАН». Этот проект направлен на укрепление сотрудничества между государствами-членами АСЕАН в области кибербезопасности, предусматривает введение в действие учебной онлайн-программы по кибербезопасности в регионе, проведение исследований по схемам сертификации в области кибербезопасности, организацию хакатонов АСЕАН и студенческих обменов в области кибербезопасности[36].

61. С 2017 по 2019 год МСЭ осуществлял проект по оказанию поддержки малым островным государствам Тихого океана в создании национальных, субрегиональных и региональных рамок кибербезопасности и повышении квалификации в этих областях. Программа была направлена на оценку готовности к созданию национальных групп реагирования на компьютерные инциденты в Папуа — Новой Гвинее, Самоа, Тонга и Вануату, а также на разработку и составление планов создания таких групп. В рамках этого проекта МСЭ провел учебные семинары для повышения осведомленности и развития навыков, в ходе которых более 200 участников и более 70 организаций обменялись опытом в области реагирования на инциденты и защиты объектов критической информационной инфраструктуры. Впоследствии результаты, полученные при подведении итогов, были сопоставлены с показателями Модели развитости потенциала

[34] См. https://www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.

[35] См. https://www.cybersec-alliance.org/camp/index.do.

[36] См. https://www.kangwon.ac.kr/english/contents.do?key=2356&.

кибербезопасности для государств, разработанной Центром глобального потенциала кибербезопасности Оксфордской школы Мартина при Оксфордском университете[37].

62. Тихоокеанская оперативная сеть по кибербезопасности[38], действующая в рамках Программы сотрудничества в области кибертехнологий и важнейших технологий в Австралии, представляет собой оперативную сеть по кибербезопасности, объединяющую региональных экспертов-практиков по кибербезопасности в Тихоокеанском регионе. Сеть ведет реестр оперативных контактных лиц по вопросам кибербезопасности и обеспечивает участников платформой для обмена информацией об угрозах кибербезопасности, предоставляет техническим экспертам возможности для обмена информацией о средствах, методах и идеях, а также способствует сотрудничеству и взаимодействию, особенно в тех случаях, когда инцидент в области кибербезопасности затрагивает весь регион.

63. Были также проведены различные двусторонние мероприятия, направленные на развитие технического потенциала. Так, программа Новой Зеландии по наращиванию потенциала кибербезопасности в Тихоокеанском регионе предусматривает оказание двусторонней поддержки тихоокеанским островным государствам в разработке национальных стратегий кибербезопасности, наращивании потенциала групп реагирования на компьютерные инциденты, повышении осведомленности, разработке законодательства о кибербезопасности и киберпреступности в соответствии с международными стандартами, а также проведении расследований и судебного преследования в соответствии с таким законодательством. Среди недавних конференций в регионе — Международный симпозиум по борьбе с киберпреступностью, состоявшийся в Республике Корея 13–15 сентября 2023 года, и Тихоокеанская конференция по наращиванию киберпотенциала и сотрудничеству, которая прошла на Фиджи 2–4 октября 2023 года.

64. В рамках Программы сотрудничества в области кибертехнологий и важнейших технологий Австралия оказывает поддержку партнерам в Тихоокеанском регионе и Юго-Восточной Азии в укреплении технического и управленческого потенциала противодействия киберугрозам[39]. Программа сотрудничества, созданная в 2016 году, была расширена в 2021 году и теперь включает в себя сотрудничество в области важнейших технологий. По состоянию на ноябрь 2023 года в рамках этой программы осуществляется поддержка 126 проектов в 21 стране региона. Эти проекты включают мероприятия по укреплению потенциала в сфере кибербезопасности, использованию технологий в поддержку экономического роста и развития, защите прав человека и демократии в Интернете, предотвращению и преследованию киберпреступлений и поддержке внедрения нормативных рамок по поощрению ответственного поведения государств при использовании информационно-коммуникационных технологий в контексте международной безопасности, одобренных Организацией Объединенных Наций. Проект «Киберлагерь», стартовавший в августе 2019 года в рамках Программы сотрудничества, был разработан для того, чтобы предоставить государственным служащим Юго-Восточной Азии практические знания и навыки по общим проблемам и возможностям.

65. Центр кибернетической компетенции стран Латинской Америки и Карибского бассейна, созданный в 2022 году при поддержке Европейского союза и расположенный в Доминиканской Республике, предлагает государствам Латинской Америки и Карибского бассейна услуги по обучению и наращиванию

[37] См. https://gcscc.ox.ac.uk/the-cmm.
[38] См. https://pacson.org/.
[39] См. https://www.internationalcybertech.gov.au/our-work/capacity-building.

потенциала в области кибербезопасности и киберпреступности. Его деятельность включает предоставление учебных материалов и курсов, повышение осведомленности и поддержку политиков по вопросам национальной кибербезопасности и цифровой трансформации, а также проведение национальных и региональных консультаций по вопросам кибербезопасности. Кроме того, были предприняты двусторонние усилия по поддержке создания национальных групп реагирования на компьютерные инциденты, включая проект Бразильского агентства по сотрудничеству, направленный на поддержку создания центра реагирования на инциденты в сфере кибербезопасности в Суринаме.

66. В период с 2016 по 2019 год в рамках программы «Глобальный потенциал кибербезопасности», финансируемой Фондом партнерства Республики Корея и Всемирного банка, межрегиональной группе из шести государств была оказана специализированная техническая помощь на национальном и региональном уровнях[40]. Все государства-участники прошли оценку по Модели развитости потенциала кибербезопасности для государств, на основе которой были подготовлены аналитические доклады, проведены занятия, семинары и оказана техническая помощь. Цель проекта — помочь государствам-участникам улучшить обстановку в плане кибербезопасности на национальном уровне с привлечением лиц, ответственных за разработку политики в области кибербезопасности, и соответствующих заинтересованных сторон. Эффективность мероприятий определялась с помощью анализа воздействия.

Дополнительные области наращивания потенциала

67. Продолжается работа по наращиванию потенциала в других сквозных и тематических областях, в том числе с упором на конкретные группы, такие как женщины, молодежь, ученые и промышленные круги. Среди других направлений — повышение осведомленности населения, обеспечение доступа к цифровым технологиям и грамотности, а также борьба с киберпреступностью.

Гендер и участие женщин

68. Учрежденная в 2020 году стипендиальная программа «Женщины в сфере международной безопасности и киберпространства» является совместной инициативой Австралии, Канады, Нидерландов (Королевства), Новой Зеландии, Соединенного Королевства и Соединенных Штатов[41]. В ее рамках оказывается поддержка участию женщин-дипломатов в соответствующих межправительственных процессах под эгидой Организации Объединенных Наций, включая сессии Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, и проводятся тренинги и семинары по навыкам ведения переговоров. Во втором наборе программы будет оказана поддержка 35 женщинам-дипломатам, представляющим страны АСЕАН, Азиатско-Тихоокеанского региона, Южной Америки и Содружества, которые примут участие в заседаниях Рабочей группы открытого состава. Кроме того, стипендиатки проходят обучение в Учебном и исследовательском институте Организации Объединенных Наций по теме многосторонних переговоров, участвуют во вводном курсе, посвященном международной безопасности в киберпространстве, и перенимают опыт старших коллег, занимающихся этими вопросами в Организации Объединенных Наций в Нью-Йорке.

[40] См. https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp.

[41] См. https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship.

69. В настоящее время МСЭ руководит программой под названием «Ее киберпути», которая способствует равной, полной и значимой представленности женщин в сфере кибербезопасности[42]. Участницы этой программы получают поддержку в развитии навыков, необходимых для участия в разработке политики в области кибербезопасности на национальном и международном уровнях, повышении осведомленности и снижении барьеров для участия женщин в этой области, а также в расширении участия и представленности женщин в составе трудовых ресурсов в области кибербезопасности. В Юго-Восточной Азии МСЭ реализовал проект по активизации разработки стандартов и рамочных программ в области важнейших технологий, которые способствуют вовлечению, участию и расширению прав и возможностей женщин. Этот проект поддерживает разработку политики, стандартов, рамок и инициатив, направленных на смягчение предвзятости и укрепление доверия и инклюзивности. Первоначально проект был развернут в Индонезии, Малайзии, Таиланде и на Филиппинах с перспективой распространения на другие государства региона.

70. МСЭ также предлагает программу наставничества для женщин в киберпространстве. Осуществление этой программы, совместно организованной МСЭ, Форумом групп оперативного реагирования и обеспечения безопасности и Глобальным партнерством в интересах гендерного равенства в цифровую эпоху (которое также называют «Партнерством равных»), в ее изначальном варианте было начато в 2021 году в Международный женский день. За время существования этой программы в обучении и передаче опыта приняли участие почти 300 женщин из 73 стран.

Привлечение молодежи и повышение осведомленности

71. Чтобы повысить осведомленность и укрепить потенциал молодежи, интересующейся безопасностью информационно-коммуникационных технологий, а также вовлечь ее, группа реагирования на компьютерные инциденты Турции провела 24-часовое онлайн-соревнование по кибербезопасности в формате «захват флага», получившее название «Киберзвезда». В 2019 году в нем приняли участие 20 000 человек, как в командном, так и в индивидуальном зачете. Группа реагирования на компьютерные инциденты также осуществляет киберпрограмму под названием «Фетих», направленную на дальнейшее развитие навыков у студентов, желающих найти себе работу в этой сфере.

72. Некоторые государства отмечают усилия на национальном уровне по повышению осведомленности о важности передового опыта в области кибербезопасности. Так, каждый октябрь Национальная гвардия Мексики проводит мероприятия в рамках национальной недели кибербезопасности, цель которой — собрать представителей всех соответствующих секторов для обмена передовым опытом и практикой в области защиты объектов важнейшей инфраструктуры, обеспечения безопасности граждан в киберпространстве, цифровой экономики, неприкосновенности частной жизни и согласования национальных законодательных рамок.

Взаимодействие с промышленностью и частным сектором

73. Государства неоднократно подчеркивали ценность государственно-частного партнерства и сотрудничества с партнерами из соответствующих секторов в деле повышения потенциала противодействия киберугрозам. Государства отметили свои усилия по проведению консультаций с ключевыми государствен-

[42] См. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/HerCyberTracks.aspx.

ными и частными организациями для оценки общего уровня национальной кибербезопасности. В октябре 2023 года на Кубанской конференции по кибербезопасности представители высших учебных заведений, государственных и муниципальных органов власти, руководители инфраструктурных предприятий и объектов Российской Федерации и члены международного сообщества обсудили вызовы, задачи и тенденции. В рамках мероприятия также прошло ориентированное на молодежь соревнование «Кубань: захват флага — 2023»[43].

74. Компания «Гугл» представила на рассмотрение государств дорожную карту кибербезопасности, разработанную с опорой на накопленный опыт и примеры передовой практики в деле создания глобальных облачных решений и решений по обеспечению безопасности для правительств и индивидуальных пользователей. Цель этой дорожной карты — поддержать государства в разработке национальных стратегий кибербезопасности для защиты объектов критически важной инфраструктуры, граждан и экономического процветания[44].

Ресурсы и исследования научно-образовательных учреждений

75. Гаагская программа по международной кибербезопасности проводит исследования в области развития цифровых технологий и кибернорм, организует ежегодные научные конференции и составляет сборники научных исследований и дебатов[45]. Недавние публикации посвящены таким темам, как участие многих заинтересованных сторон в процессах нормотворчества в области кибербезопасности и ответственное поведение в киберпространстве.

76. В Модели развитости потенциала кибербезопасности для государств дается определение пяти критериев развитости кибербезопасности и шаги, необходимые для соответствия им. С 2015 года эта модель использовалась более 130 раз в более чем 90 государствах при содействии Центра глобального потенциала кибербезопасности в сотрудничестве с международными организациями, региональными и другими партнерскими организациями. В перспективе Центр глобального потенциала кибербезопасности разрабатывает дополнительный параметр в рамках Модели для измерения потенциала искусственного интеллекта, чтобы поддержать государства в адаптации к искусственному интеллекту и его безопасному и устойчивому использованию.

Развитие цифровых технологий, доступ к ним и грамотность

77. Программа развития Организации Объединенных Наций (ПРООН) реализует целый ряд инициатив, направленных на поддержку создания цифровой инфраструктуры, повышение уровня цифровой грамотности или внедрение решений в области электронного управления[46]. ПРООН ввела оценку готовности к цифровым технологиям с целью выявления и определения приоритетности мероприятий в области цифровых технологий в рамках пути цифровой трансформации страны. Эта оценка позволяет определить текущий цифровой контекст страны — от ситуации, когда базовые цифровые основы могут отсутствовать или быть неполными, до ситуации, когда цифровые технологии поставлены в центр национального роста и развития (так называемые стадии цифровой готовности).

78. Программа цифрового доступа правительства Соединенного Королевства Великобритании и Северной Ирландии направлена на стимулирование более

[43] См. https://kubcsc.ru/#events.
[44] См. https://safety.google/intl/en_uk/.
[45] См. https://www.thehagueprogram.nl/.
[46] См. https://www.undp.org/digital.

инклюзивного, доступного, безопасного и надежного цифрового доступа для сообществ Бразилии, Индонезии, Кении, Нигерии и Южной Африки[47].

79. Правительства Джибути, Кении и Сомали получают поддержку по линии Инициативы по созданию цифрового правительства и обеспечению кибербезопасности в странах Африканского Рога, направленную на укрепление электронного правительства и развитие электронных услуг с упором на нужды людей. В июле 2023 года Буркина-Фасо в партнерстве с Альянсом «Умная Африка» по линии Цифровой академии «Умная Африка» организовала сертификационные учебные курсы по облачным вычислениям и кибербезопасности.

80. Инициатива МСЭ “Cyber4Good” направлена на облегчение доступа к цифровым услугам и инструментам в наименее развитых странах при участии представителей частного сектора и при поддержке Республики Корея[48]. Одним из результатов этого проекта станет создание Фонда развития кибербезопасности МСЭ, действующего в соответствии с моделью управления и под руководством консультативного совета. Программа Европейского союза «Потенциал противодействия киберугрозам в целях развития» оказывает государственным и частным структурам поддержку в деле укреплении кибербезопасности и потенциала противодействия киберугрозам в глобальном масштабе[49].

81. Программа Всемирного банка «Партнерство в области развития цифровых технологий» призвана поддержать инклюзивные цифровые преобразования в более чем 80 странах мира[50]. Многосторонний донорский целевой фонд кибербезопасности, созданный в 2021 году при поддержке Германии, Нидерландов (Королевство), Эстонии и Японии, содействует программе цифрового развития путем проведения исследований, поддержки программ, оценки и снижения рисков для объектов критически важной инфраструктуры и секторов с высоким уровнем риска. В сотрудничестве с Африканским союзом инициатива Всемирного банка «Цифровая экономика для Африки» направлена на поддержку реализации Стратегии цифровой трансформации Африканского союза на 2020–2030 годы. Сквозной темой этой стратегии, которая опирается на такие основополагающие компоненты, как цифровая инфраструктура, услуги, навыки, благоприятная политическая и нормативная среда, инновации и предпринимательство, стали кибербезопасность, конфиденциальность и защита персональных данных. В ней изложены подробные предложения по наращиванию потенциала в области цифрового развития, цифрового доступа и цифровой грамотности, включая содействие укреплению человеческого и институционального потенциала путем проведения информационно-просветительских кампаний, профессиональной подготовки, исследований и разработок, а также создания групп реагирования на компьютерные инциденты[51].

Борьба с киберпреступностью

82. В 2013 году в Управлении Организации Объединенных Наций по наркотикам и преступности была создана Глобальная программа борьбы с киберпреступностью. Ее мандат изложен в резолюции 65/230 Генеральной Ассамблеи и резолюциях 22/7 и 22/8 Комиссии по предупреждению преступности и уголовному правосудию. Глобальная программа действует на основе этих резолюций, при этом следует отметить, что в настоящее время Генеральная Ассамблея ведет

[47] См. https://www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982/.
[48] См. https://www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119.
[49] См. https://cyber4dev.eu/.
[50] См. https://www.digitaldevelopmentpartnership.org/.
[51] См. https://www.worldbank.org/en/programs/all-africa-digital-transformation.

переговоры о заключении договора. В программе рассматриваются взаимосвязанные аспекты борьбы с киберпреступностью: предупреждение, выявление, расследование, судебное преследование и вынесение приговора или решения.

83. В настоящее время Международная организация уголовной полиции (Интерпол) через свой многосторонний Кибернетический информационно-аналитический центр руководит разработкой программ по оказанию технической помощи правоохранительным органам и наращиванию их потенциала в области информационно-коммуникационных технологий и киберпреступности, а также осуществлением таких программ. Кибернетический информационно-аналитический центр помогает странам-участницам выявлять киберугрозы, разрабатывать стратегии по их предотвращению и пресечению, а также координировать ответные действия на эти угрозы.

Противодействие использованию информационно-коммуникационных технологий в террористических целях

84. Глобальная контртеррористическая программа по кибербезопасности и новым технологиям помогает государствам-членам и международным и региональным организациям разрабатывать и осуществлять эффективные меры реагирования на возникающие вызовы и возможности, связанные с использованием информационно-коммуникационных технологий в борьбе с терроризмом. Эта программа направлена на развитие знаний и повышение осведомленности, а также на совершенствование навыков и потенциала, необходимых для осуществления стратегических мер реагирования, защиты объектов критически важной инфраструктуры от террористической деятельности с использованием информационно-коммуникационных технологий и укрепления потенциала системы уголовного правосудия. В рамках программы, через которую прошли более 4000 должностных лиц из 150 государств-членов, было проведено более 60 семинаров по наращиванию потенциала и опубликовано 12 информационных материалов. Кроме того, эта программа также позволила оказать помощь в укреплении потенциала в области кибербезопасности в форме проведения контртеррористических киберучений и тренировочных занятий.

V. Замечания и выводы Секретариата

85. Наращивание потенциала в области информационно-коммуникационных технологий в контексте международной безопасности по праву остается в числе самых приоритетных задач государств. Наращивание потенциала во многом определяет усилия, предпринимаемые по всем смежным вопросам, рассматриваемым Рабочей группой открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ 2021–2025, а именно: устранение существующих и новых угроз и анализ применимости международного права к использованию государствами таких технологий и поддержке мер укрепления доверия. Многие государства также подчеркнули важность рассмотрения вопроса о наращивании потенциала в рамках любого будущего регулярного институционального диалога под эгидой Организации Объединенных Наций по вопросам безопасности информационно-коммуникационных технологий. **В этой связи наращивание потенциала должно оставаться одним из основных и сквозных элементов всех соответствующих обсуждений государствами в Организации Объединенных Наций вопроса о безопасности в контексте информационно-коммуникационных технологий. Достижение прогресса во всех соответствующих областях — от норм международного права до мер укрепления доверия — потребует выделения ресурсов для осуществления соответствующих мер по наращиванию потенциала.**

86. Генеральный секретарь подчеркнул исключительную важность инвестирования в развитие цифровой грамотности и цифровой инфраструктуры для устранения цифрового разрыва (A/75/982). Кроме того, государства вновь подчеркнули, что преимуществами цифровых технологий пользуются не все в равной степени, и, соответственно, отметили необходимость уделить должное внимание растущему цифровому разрыву в контексте ускорения реализации целей в области устойчивого развития, учитывая при этом национальные потребности и приоритеты государств. **Как следствие, крайне важно, чтобы наращивание потенциала в области информационно-коммуникационных технологий оптимально отвечало потребностям и приоритетам всех государств, особенно развивающихся стран, с целью устранения цифрового разрыва, в том числе гендерного цифрового разрыва. Кроме того, усилия по наращиванию потенциала должны способствовать устойчивому развитию.**

87. Влияние стремительного научно-технического прогресса на международный мир и безопасность еще не до конца изучено. Ожидается, что возможности и риски, создаваемые стремительным развитием новых технологий, включая искусственный интеллект и квантовые технологии, окажут глубокое влияние на потребности и приоритеты государств в области наращивания потенциала на техническом и директивном уровнях. С одной стороны, использование возможностей информационно-коммуникационных технологий, таких как расширенное обнаружение и анализ угроз, автоматизированное реагирование на инциденты, расширенное обнаружение вредоносных программ, а также средства обнаружения и предотвращения мошенничества, требует увеличения потенциала. С другой стороны, усилия по наращиванию потенциала крайне важны для того, чтобы государства обладали необходимыми знаниями и навыками для решения таких проблем, как злонамеренная деятельность в области информационно-коммуникационных технологий с использованием искусственного интеллекта, предвзятость и дискриминация, присущие системам искусственного интеллекта, и вопросы транспарентности. **Конкретные инициативы по наращиванию потенциала могут быть направлены на повышение уровня грамотности и знаний о воздействии этих новых технологий, разработку национальных стратегий ответственного проектирования, разработки и использования новых технологий, а также механизмов международного сотрудничества для повышения потенциала противодействия киберугрозам путем передачи знаний, примеров передового опыта и извлеченных уроков.**

88. Постоянной проблемой, препятствующей эффективным и устойчивым усилиям по наращиванию потенциала, остается возможное дублирование. В этой связи стоит отметить, что в решении 630 Совета Международного союза электросвязи, принятом в августе 2023 года, МСЭ было поручено разработать ресурс для государств-членов, включающий, в частности, информацию о реализуемых им программах по наращиванию потенциала, а также о других соответствующих программах[52]. Этот ресурс предлагается обновлять с учетом новых задач и событий. Государства регулярно поднимают вопрос об использовании синергетического эффекта и применении существующих инициатив в этой области. **Учитывая универсальный характер Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ, государствам рекомендуется использовать специальный межправительственный процесс для дальнейшего изучения вопроса о том, как избежать дублирования в целях обеспечения наиболее эффективного подбора ресурсов для удовлетворения потребностей.**

[52] Доступно на сайте https://www.itu.int/md/S23-CL-C-0124/en.