Организация Объединенных Наций A/77/92

Генеральная Ассамблея

Distr.: General
8 June 2022
Russian
Original: Arabic/English/Russian/
Spanish

Семьдесят седьмая сессия
Пункт 94 первоначального перечня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий

Доклад Генерального секретаря

Содержание

* A/77/50.

22-08761 (R) 210722 270722

I. Введение

1. 6 декабря 2021 года Генеральная Ассамблея приняла резолюцию 76/19 «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности и поощрение ответственного поведения государств в сфере использования информационно-коммуникационных технологий» по пункту 95 повестки дня «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

2. В пункте 6 резолюции 76/19 Генеральная Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

a) усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области;

b) содержание концепций, упомянутых в докладе Рабочей группы открытого состава и докладах Группы правительственных экспертов.

3. Во исполнение этой просьбы 24 января 2022 года всем государствам-членам была направлена вербальная нота с предложением представить информацию по этому вопросу.

4. Ответы, полученные на момент составления настоящего доклада, содержатся в разделах II и III. Дополнительные ответы, полученные после 31 мая 2022 года, будут опубликованы на веб-сайте Управления по вопросам разоружения (www.un.org/disarmament/ru/достижения-в-сфере-информатизации-и-т/) на том языке, на котором они были представлены.

II. Ответы, полученные от правительств

Армения

[Подлинный текст на английском языке]
[31 мая 2022 года]

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству

Правительство Армении создало совет по цифровизации, призванный стимулировать развитие цифровых навыков и цифровизацию системы государственного управления и экономики. По данным на 2021 год было обсуждено около 25 программ и стратегических документов, велась непрерывная работа в области цифровой идентификации, подтверждения подлинности официальных документов, электронных лицензий, внедрения практики индивидуальных и публичных уведомлений, внедрения единых систем электронного правосудия, а также по ряду других направлений цифровой повестки дня.

11 февраля 2021 года Республика Армения утвердила стратегию цифровизации. Эта стратегия предусматривает цифровую трансформацию правительства, экономики и общества путем внедрения и развития инновационных технологий, кибербезопасности, политики данных, электронных услуг и систем электронного правительства, координации процессов цифровизации, определения общих стандартов и цифровой среды, а также инициатив, содействующих использованию цифровых технологий в частном секторе экономики, и разработки и реализации программ, способствующих применению электронных инструментов населением.

В рамках стратегии цифровизации Армении на период 2021–2025 годов планируется осуществить следующие инициативы:

a) внести законодательные и нормативно-правовые поправки в сфере информационной безопасности;

b) разработать концепцию государственной политики в области открытых данных;

c) провести занятия по кибербезопасности для жителей приграничных деревень (в настоящее время курсы по кибербезопасности проводятся для государственных служащих);

d) создать национальный центр кибербезопасности. В частности, рассматривается возможность введения критериев кибербезопасности, создания государственных групп оперативного реагирования и проведения общественно-просветительских мероприятий, направленных на повышение грамотности в области кибербезопасности.

Министерство высокотехнологичной промышленности планирует разработать комплексную политику и план действий по преодолению вызовов в области кибербезопасности, включая процесс создания центра кибербезопасности, формирование механизмов управления рисками и быстрого реагирования в условиях стихийных бедствий, чрезвычайных ситуаций и военного положения.

Министерство подчеркивает важность тесного сотрудничества с частным сектором, межведомственного взаимодействия, локализации международного опыта, а также соблюдения международных стандартов кибербезопасности, межгосударственного сотрудничества и членства в международных структурах безопасности.

Армения, совместно с международными и региональными организациями, разрабатывает политику и развивает потенциал в области кибербезопасности, в том числе посредством участия соответствующих армянских учреждений в различных тематических семинарах, конференциях и учебных занятиях.

Республика Армения является участником Конвенции Совета Европы о киберпреступности. Совсем недавно Армения инициировала национальную процедуру подписания Второго дополнительного протокола к Конвенции Совета Европы о расширении сотрудничества и раскрытии электронных доказательств.

Армения активно вовлечена в усилия Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Рабочая группа имеет уникальную возможность закладывать основу для новых стандартов в области информационно-коммуникационных технологий (ИКТ).

Сотрудничество в рамках проекта Совета Европы «КиберВосток» направлено на наращивание потенциала экспертов армянских государственных учреждений в деле противодействия угрозам киберпреступности.

Армения также высоко ценит постоянные усилия по укреплению доверия в информационно-коммуникационной сфере в рамках Организации по безопасности и сотрудничеству в Европе, которая способствует повышению прозрачности, предсказуемости и стабильности в этой области.

В то же время следует отметить сотрудничество с наднациональными компаниями. В Армении расположены подразделения ведущих ИТ-компаний, таких как «Синопсис», «Ментор графикс», «Нэшнл инструментс», «Майкрософт», «ВМвэр», «Д-Линк», «Оракл», «Циско» и других. Компании «Майкрософт» и «Циско» регулярно оказывают содействие или участвуют в форумах, чтобы помочь правительству Армении ознакомиться с последними разработками в области кибербезопасности и обороны.

Австралия

[Подлинный текст на английском языке]
[31 мая 2022 года]

В ответ на содержащуюся в резолюции 76/19 Генеральной Ассамблеи просьбу Австралия приветствует возможность поделиться с Генеральным секретарем своими взглядами на поощрение ответственного поведения государств в киберпространстве. Настоящая информация подготовлена на основе данных, представленных Австралией в мае 2021 года в ответ на ранее принятые резолюции Генеральной Ассамблеи[1], включая недавнюю резолюцию (см. A/76/187). Австралия призывает все государства активно участвовать в предоставлении регулярных обновлений Генеральному секретарю, чтобы повысить прозрачность и углубить понимание усилий друг друга по продвижению ответственного поведения государств в киберпространстве.

Рамки ответственного поведения государств в киберпространстве

В целом в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2010, 2013 и 2015 годы[2] подтверждаются применимость и необходимость существующих норм международного права в контексте поддержания мира и стабильности в киберпространстве. В этих докладах также сформулированы 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств и отмечена необходимость принимать меры по укреплению доверия и координировать работу по наращиванию потенциала. В совокупности эти четыре принципа часто называют рамками ответственного поведения государств в киберпространстве.

Австралия с удовлетворением отметила, что в датированном мартом 2021 года докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/75/816), который был обсужден и одобрен всеми 193 государствами-членами Организации Объединенных Наций, отражена всеобщая приверженность этому рамочному документу. Австралия с удовлетворением отметила также, что в работе шестой Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности принял участие ведущий эксперт, предоставивший дополнительные практические рекомендации по реализации этого рамочного документа

[1] Резолюции 65/41, 68/243, 70/237, 74/28 и 75/32.
[2] Соответственно A/65/201, A/68/98 и A/70/174.

(см. A/76/135), которые впоследствии были одобрены Генеральной Ассамблеей в ее резолюции 76/19.

Австралия подтверждает свое обязательство действовать в соответствии со сводными докладами Группы правительственных экспертов и докладом Рабочей группы. Австралия по-прежнему активно участвует в деятельности Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы), созданной в соответствии с резолюцией 75/240, и является идейным соавтором предложения Франции и Египта о создании программы действий. Австралия поддерживает создание программы действий, в рамках которой будет функционировать постоянный, инклюзивный и транспарентный форум для непрерывного обсуждения и осуществления практических действий по кибервопросам под эгидой Организации Объединенных Наций.

В интересах транспарентности Австралия вскоре опубликует обновленную информацию о том, как она внедряет и соблюдает 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств. Хотя эти нормы не заменяют и не изменяют обязательства или права государств по международному праву, которые носят обязательный характер, Австралия подтверждает, что упомянутые 11 норм применяются совместно с нормами международного права и содержат дополнительные конкретные указания в отношении того, что представляет собой ответственное поведение государств при использовании информационно-коммуникационных технологий. В ближайшем будущем Австралия также разместит на портале по вопросам киберполитики Института Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР) результаты своей первоначальной самооценки выполнения обязательств Организации Объединенных Наций в области киберпространства, осуществленной в рамках национального опроса Института. Австралия рекомендует всем государствам использовать формат национального опроса и призывает государства рассмотреть возможность размещения результатов своих самооценок в открытом доступе. Наблюдение за выполнением рекомендаций Организации Объединенных Наций дает ряд преимуществ. Так, государства могут определить, как они внедрили свод норм, где могут быть пробелы во внедрении и есть ли какие-либо препятствия на его пути. В свою очередь, это может принести пользу при разработке целевых программ сотрудничества и наращивания потенциала, которые могут потребоваться для устранения каких-либо выявленных пробелов в потенциале и/или барьеров в ходе реализации.

Международное право

Австралия призывает все государства продолжать изучать то, как международное право применяется к поведению государств в киберпространстве, и поддерживать транспарентность своих позиций в этой связи. Мы вновь заявляем, что даже в случае расхождения мнений, развитие понимания позиций друг друга в отношении применения международного права в киберпространстве повышает предсказуемость и снижает риск просчетов, которые могут привести к эскалации ситуации, связанной с поведением государств. Австралия вновь заявляет, что международное право наиболее эффективно в том случае, когда государства внедряют и выполняют свои правовые обязательства международного характера и, при необходимости, сотрудничают в деле поддержания международного права и обеспечения ответственности за его нарушения.

Австралия приветствовала выводы, содержащиеся в докладе Группы правительственных экспертов за 2021 год (A/76/135), о том, что международное гуманитарное право применимо к деятельности в киберсреде в ситуациях вооруженного конфликта.

Позиция Австралии относительно применения международного права к поведению государств в киберпространстве представлена в ряде следующих документов:

- представленная Австралией в 2021 году информация, которая вошла в официальный сборник добровольно представляемых национальных материалов по вопросу о том, как международное право применяется к использованию информационно-коммуникационных технологий государствами, предоставленных участвующими правительственными экспертами, входящими в Группу правительственных экспертов (A/76/136);
- стратегия международного взаимодействия в киберпространстве и по вопросам критически важных технологий 2021 года;
- тематические исследования по применению международного права в киберпространстве 2020 года (представлены Рабочей группе открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности);
- Дополнение по вопросам международного права 2019 года;
- международная стратегия кибервзаимодействия 2017 года.

В дополнение к участию Австралии в процессах Организации Объединенных Наций по вопросам применения международного права в киберпространстве, Австралия старается также участвовать в подобных дискуссиях на региональных форумах. В этой связи в конце 2021 года Австралия выступила с заявлением на пятьдесят девятой ежегодной сессии Афро-азиатской консультативно-правовой организации по международному праву в киберпространстве.

Сдерживание безответственного поведения государства и реагирование на него

Австралия не потерпит деятельности, которая наносит ущерб международному миру и стабильности или противоречит согласованному всеми государствами — членами Организации Объединенных Наций рамочному документу, в киберпространстве. Австралия призывает мировое сообщество проливать свет на злонамеренную активность с использованием киберсредств и привлекать виновных к ответственности. Австралия проводит политику публичного указания источника злонамеренной активности с использованием киберсредств в тех случаях, когда он известен и когда это отвечает нашим интересам. Эта политика не направлена против какой-либо конкретной страны. На сегодняшний день Австралия публично указывала на источники злонамеренной активности с использованием киберсредств в 13 случаях. Совсем недавно, 10 мая 2022 года, Австралия присоединилась к Соединенным Штатам Америки и Европейскому союзу, присвоив в ряде случаев разрушительную, подрывную и дестабилизирующую активность с использованием киберсредств против Украины российскому правительству.

Взаимодействие с участием различных заинтересованных сторон

Австралия благодарит председателя Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы) Бурхана Гафура за его конструктивные усилия по достижению

консенсусного согласия по ряду прозрачных и сбалансированных условий будущего участия неправительственных заинтересованных сторон в деятельности Рабочей группы. Австралия надеется, что эти условия будут официально утверждены в ходе третьей основной сессии Рабочей группы, которая состоится в июле 2022 года. Австралия является убежденной сторонницей участия различных заинтересованных сторон в обсуждении ответственного поведения государств в киберпространстве. Киберпространство уникально: представителям частного сектора, технического сообщества, гражданского общества и научно-академических кругов отводится жизненно важная роль в техническом управлении и руководстве им, и сообщество различных заинтересованных сторон может поделиться мнениями, которые позволят нам лучше понять возникающие киберугрозы, их воздействие и способы их устранения. Австралия была разочарована попытками некоторых государств помешать участию заинтересованных сторон в этом процессе, что, по нашему мнению, противоречит принципам, в соответствии с которыми была создана эта Рабочая группа. Австралия считает, что деятельность Рабочей группы может оказать далеко идущее воздействие на многие заинтересованные стороны, включая прямое воздействие на сообщества и отдельных людей, и что устранение исходящих из киберпространства угроз требует от нас использования опыта, знаний и ресурсов всех соответствующих заинтересованных сторон. В этой связи Австралия приветствует согласованные условия как шаг к прозрачности и инклюзивности.

Женщины в киберпространстве

Как признается в повестке дня по вопросу о женщинах и мире и безопасности, конфликты и кризисы оказывают особое, несоразмерно большое воздействие на женщин и девочек, которые, кроме того, недопредставлены в международных процессах обеспечения мира и безопасности, а порой и исключены из них. Как отмечается в отчете ЮНИДИР “Still behind the curve: gender balance in arms control, non-proliferation and disarmament diplomacy” («Сохраняющееся отставание: гендерный баланс в сфере дипломатии в области контроля над вооружениями, нераспространения и разоружения»), в Первом комитете наблюдается значительное отставание по сравнению с мерами, предпринимаемыми во всех других комитетах Организации Объединенных Наций для достижения гендерного паритета. Данные ЮНИДИР показывают, что женщины составляют 27 процентов выступающих в ходе прений Первого комитета. Этот показатель снижается в среднем до 20 процентов на форумах, посвященных более специализированным темам.

Для решения этой проблемы в феврале 2020 года Австралия совместно с Канадой, Нидерландами, Новой Зеландией, Соединенным Королевством Великобритании и Северной Ирландии и Соединенными Штатами учредила стипендиальную программу «Женщины в сфере международной безопасности и киберпространства». Эта стипендиальная программа обеспечивает обучение женщин-дипломатов начального и среднего звена по теме многосторонних переговоров, киберполитики и международного права, а также позволяет спонсировать поездки в Нью-Йорк для участия их национальных делегаций в заседаниях Организации Объединенных Наций, на которых рассматриваются вопросы ответственного поведения государств в киберпространстве, в том числе в рамках деятельности Рабочей группы.

Австралия рада, что благодаря этой программе многие стипендиатки смогли присоединиться к своим национальным делегациям на первой и второй сессиях Рабочей группы и внесли значительный вклад в ее работу и в продвижение повестки дня по вопросу о женщинах и мире и безопасности. В ходе первой сессии Рабочей группы, состоявшейся в декабре 2021 года, женщины

составили 37 процентов выступавших. В ходе второй сессии, состоявшейся в марте 2022 года, женщины составили 43 процента выступавших и половину всех выступавших на тему международного права.

Азербайджан

[Подлинный текст на английском языке]
[31 мая 2022 года]

За последние годы в Азербайджане было принято несколько новых законодательных актов, направленных на обеспечение информационной безопасности. Кроме того, в соответствии с указами и распоряжениями президента Азербайджана были приняты концепция развития, стратегическая «дорожная карта», национальная стратегия и государственные программы и было налажено сотрудничество с различными странами.

Ввиду необходимости уделять приоритетное внимание безопасности критически важной информационной инфраструктуры был принят нормативно-правовой акт, направленный на усиление безопасности в этой сфере. В вышеупомянутом правовом акте учтены классификация этих объектов инфраструктуры по степени их важности и определение общих и специальных требований безопасности, а также предусмотрен постоянный контроль с применением соответствующих методов.

В 2018 году в соответствии с распоряжением Президента Азербайджана был создан Координационный комитет по информационной безопасности.

В соответствии с указом Президента Азербайджана от 17 апреля 2021 года для поддержания безопасности критически важной информационной инфраструктуры было определено разделение полномочий между учреждениями.

В целях укрепления человеческого капитала в этой области Киберакадемия Министерства цифрового развития и транспорта организовала различные тренинги с выдачей сертификатов государственного и международного образца.

В рамках совместных программ «КиберВосток» и «Кибербезопасность — Восток» Европейского союза и Совета Европы международные эксперты провели для представителей соответствующих государственных органов Азербайджана виртуальные семинары по защите персональных данных, противодействию киберпреступности и работе с электронными доказательствами.

В рамках стипендиальной программы Корейского агентства по международному сотрудничеству представители нескольких государственных органов Азербайджана прошли первый сертифицированный учебный курс по кибербезопасности.

В дополнение к вышеупомянутому, были организованы консультации и инициативы по сотрудничеству с группами реагирования на компьютерные инциденты различных государств.

В Глобальном индексе кибербезопасности за 2020 год Международного союза электросвязи Азербайджан занимает сороковое место в мире и третье место (после Российской Федерации и Казахстана) в Содружестве Независимых Государств.

В связи с увеличением количества киберугроз в период пандемии коронавирусного заболевания (COVID-19), а также выявленными недостатками программного и технического оборудования на сайте www.cert.az и в социальных

сетях были размещены соответствующие уведомления и сообщения о методах защиты от киберугроз.

Куба

[Подлинный текст на испанском языке]
[31 мая 2022 года]

Ненадлежащее использование информационно-телекоммуникационных технологий по-прежнему вызывает серьезную озабоченность международного сообщества, что обусловливает необходимость борьбы с растущими угрозами в этой области.

Мы осуждаем ненадлежащее использование медиаплатформ, включая социальные сети и радиопередачи, в качестве инструмента вмешательства с помощью пропаганды языка вражды, подстрекательства к насилию, подрывной деятельности, дестабилизации, распространения фальшивых новостей и искажения действительности в политических целях и в качестве предлога для развязывания войны, угрозы силой или ее применения в нарушение целей и принципов Устава Организации Объединенных Наций и международного права.

В этой связи мы отвергаем нетрадиционные методы ведения войны, применяемые правительством Соединенных Штатов против Кубы, в том числе с применением новых информационных технологий и других цифровых платформ для дестабилизации и дискредитации нашей страны.

Мы вновь подтверждаем право и обязанность государства бороться, что входит в конституционные полномочия, против распространения фальшивых или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств или как наносящие ущерб укреплению мира, сотрудничества и дружественных отношений между государствами и нациями.

Мы не можем игнорировать тот факт, что растущее развитие оборонных возможностей и операций в киберпространстве может превратить его в новую зону конфликта. Мы отвергаем попытки приравнять злонамеренное использование информационно-коммуникационных технологий к понятию «вооруженное нападение», чтобы оправдать осуществление права на самооборону, предусмотренного статьей 51 Устава Организации Объединенных Наций.

Мы отвергаем преднамеренное использование этих технологий для нанесения ущерба жизненно важной инфраструктуре других государств, включая их информационные системы, или для создания иных препятствий для использования и функционирования критически важной инфраструктуры, которая необходима для социальной стабильности и безопасности государств.

Организация Объединенных Наций является ведущим многосторонним форумом и основной платформой для решения проблем в области безопасности и использования информационно-коммуникационных технологий, вызывающих обеспокоенность государств-членов. В этой связи Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы), учрежденная в соответствии с резолюцией 75/240 Генеральной Ассамблеи, является единственным доступным государствам-членам инклюзивным механизмом для обсуждения вопросов кибербезопасности на транспарентной и равноправной основе.

Мы подтверждаем важность деятельности вышеупомянутой Рабочей группы и надеемся, что этот межправительственный процесс будет способствовать заполнению существующего правового вакуума обязательными нормами, ведущими к принятию всеобъемлющего правового документа по информационно-коммуникационным технологиям в контексте международной безопасности.

Хотя меры укрепления доверия являются полезным инструментом, сами по себе такие меры не гарантируют исключительно мирного использования информационно-коммуникационных технологий, учитывая отсутствие соответствующего юридически обязывающего документа в этой области.

Куба, будучи членом Движения неприсоединившихся стран, вновь призывает развитые страны и соответствующие международные структуры предоставлять развивающимся странам, по их просьбе, помощь и сотрудничество, в том числе в форме финансовых ресурсов, наращивания потенциала и передачи технологий, с учетом конкретных потребностей и особенностей каждого государства-получателя.

Мы выступаем против применения односторонних принудительных мер, которые, подобно экономической, торговой и финансовой блокаде, введенной правительством Соединенных Штатов против Кубы, препятствуют всеобщему доступу и мирному использованию и применению информационно-коммуникационных технологий в интересах благосостояния нашего населения или ограничивают их.

Дания

[Подлинный текст на английском языке]
[31 мая 2022 года]

В Дании, как и во многих других странах мира, цифровые решения представляют собой неотъемлемую часть повседневной жизни. Они являются не только платформой для основных видов деятельности общества, но и ключевым фактором экономического роста. Однако вместе со все большей взаимосвязанностью наших обществ и цифровой инфраструктуры возросли и способность и готовность государственных и негосударственных субъектов осуществлять злонамеренную активность с использованием киберсредств. Это должно вызывать озабоченность на глобальном уровне, поскольку злонамеренная активность в киберпространстве может представлять собой противоправно-правовое деяние и привести к потенциальной эскалации, что, в свою очередь, угрожает международной безопасности и стабильности. Неспровоцированное и незаконное вторжение России на Украину, которое также включает кибератаки на критически важную инфраструктуру, вызывает особую озабоченность и абсолютно неприемлемо, поскольку представляет собой нарушение международного права и подрывает принципы рамок ответственного поведения государств в киберпространстве.

Дания, будучи одной из наиболее цифровизированных стран мира, все так же преисполнена решимости соответствующим образом предотвращать и пресекать злонамеренную активность с использованием киберсредств и реагировать на инциденты в области информационной безопасности, а также расширять международное сотрудничество в этой области. Дания, вместе с Европейским союзом, стремится укреплять международное сотрудничество в интересах формирования глобального, открытого, стабильного, мирного и безопасного киберпространства, в котором в полной мере соблюдались бы права человека, основные свободы и верховенство права. В этой связи Дания подчеркивает важность

соблюдения государствами свода норм ответственного поведения государств в киберпространстве, который позволяет поддерживать основанный на правилах международный порядок и подтверждает применимость международного права, соблюдение добровольных норм ответственного поведения государств, а также разработку и внедрение практических мер укрепления доверия. Роль этого свода норм в качестве краеугольного камня усилий международного сообщества по сдерживанию безрассудного и безответственного поведения государств в киберпространстве и предотвращению наиболее пагубных кибератак и потенциальных эскалаций неоднократно подтверждалась всеми членами Генеральной Ассамблеи. В этой связи мы призываем все государства-члены, включая Российскую Федерацию, выполнять свои обязательства.

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

На сегодняшний день Дания предприняла ряд шагов по укреплению своей кибернетической и информационной безопасности и развитию международного сотрудничества в области кибербезопасности. Датское оборонное соглашение на период 2018–2023 годов предусматривает, что на цели укрепления кибербезопасности и кибероборо ны будет выделено 1,4 млрд датских крон, что позволит усилить потенциал противодействия и устойчивость датского общества к кибератакам.

Наряду с датской стратегией в области кибернетической и информационной безопасности на 2018–2021 годы были представлены 25 инициатив, а также 6 специальных стратегий с целью:

a) повысить кибернетическую и информационную безопасность, особенно в критически важных секторах;

b) обеспечить систематичность и скоординированность усилий;

c) повысить технологическую устойчивость цифровой инфраструктуры;

d) повысить осведомленность граждан, деловых кругов и органов власти в вопросах кибербезопасности.

В рамках этой стратегии в шести критически важных секторах (энергетика, финансы, транспорт, здравоохранение, телекоммуникации и морское судоходство) были созданы специализированные подразделения по кибернетической и информационной безопасности, а также форумы для обмена опытом между этими подразделениями.

Центр кибербезопасности также создал Академию киберзащиты — отдельное подразделение, на базе которого проводятся курсы интенсивной подготовки, и оказывает широкую поддержку образовательным и исследовательским программам в области кибербезопасности. Аналогичным образом Агентство по работе электронного правительства разработало несколько учебных курсов, методических материалов и мероприятий по кибербезопасности и информационной безопасности, предназначенных для сотрудников высшего руководящего звена, специалистов в области кибербезопасности и государственных служащих.

Кроме того, Агентство по электронному правительству разработало вебсайт www.sikkerdigital.dk, который содержит конкретные рекомендации для граждан по кибербезопасности и информационной безопасности и проводит национальные кампании по обучению навыкам безопасного поведения в цифровом пространстве, которые проводятся в сотрудничестве с муниципальными и региональными властями.

В Дании был создан государственно-частный Совет кибербезопасности (“Cybersikkerhedsråd”), который консультирует правительство по вопросам укрепления кибербезопасности и улучшения обмена знаниями между органами власти и деловыми и научно-исследовательскими кругами. Наконец, наряду с реализацией Датской стратегии в области кибербезопасности и информационной безопасности на 2018–2021 годы, Дания также укрепила свое международное сотрудничество в киберсфере, что позволило этой стране активизировать свое участие в межгосударственных киберфорумах, проводимых на базе таких структур, как Организация Объединенных Наций, Европейский союз, Организация Североатлантического договора (НАТО) и Организация по безопасности и сотрудничеству в Европе (ОБСЕ).

В декабре 2021 года правительство страны представило новую национальную стратегию кибернетической и информационной безопасности на 2022–2024 годы. В рамках этой стратегии текущие усилия по укреплению кибербезопасности и информационной безопасности будут продолжены и расширены посредством реализации 34 основных инициатив, нацеленных на работу с государственным и частным секторами, а также с датскими гражданами в целом. В целом в стратегии намечены четыре основные цели:

a) во-первых, стратегия дополнительно укрепляет потенциал противодействия критически важной информационно-коммуникационной инфраструктуры, которая поддерживает жизненно важные функции общества. Для обеспечения надлежащего уровня кибербезопасности как государственных учреждений, так и бизнеса был предпринят ряд стратегических мер, включая ужесточение требований безопасности к управлению государственными системами в сфере информационно-коммуникационных технологий, критически важными для общества, и усиление предпринимаемых полицией мер по борьбе с киберпреступностью. В стратегии также расширяется число критически важных секторов с охватом более широкого круга государственных учреждений, которые отвечают за обеспечение жизненно важных общественных функций с использованием информационных технологий. В дополнение к минимальным требованиям, которые ранее были включены в стратегию на 2018–2021 годы, государственные учреждения в этих критически важных секторах обязаны соблюдать ряд особых требований безопасности. Это необходимо для того, чтобы министерства, несущие особую ответственность за обеспечение жизненно важных функций общества, были способны быстро и эффективно действовать в случае серьезного инцидента в области кибербезопасности;

b) во-вторых, стратегия включает в себя ряд инициатив, направленных на укрепление навыков кибербезопасности у датских граждан и повышение приверженности руководства укреплению кибербезопасности. Среди инициатив — новые специализированные программы обучения для государственных служащих, а также образовательные программы, которые дают детям, молодежи и взрослым возможность освоить навыки цифровой грамотности. Кроме того, к высшему руководству и лидерам применяются повышенные требования и ожидания в отношении определения приоритетности кибербезопасности и информационной безопасности;

c) в-третьих, эта стратегия направлена на укрепление сотрудничества в области кибербезопасности и информационной безопасности между государственным и частным секторами. Способность обмениваться знаниями и опытом между секторами крайне важна для достижения высокого уровня кибербезопасности и информационной безопасности. По этой причине в целях расширения возможностей Центра кибербезопасности по предоставлению рекомендаций будут созданы «горячая линия» по кибербезопасности, по которой можно будет

легко получить консультацию на тему киберпреступности, а также специальное подразделение по кибербезопасности для малых и средних предприятий;

d) в-четвертых, эта стратегия направлена на дальнейшее укрепление международных усилий Дании в области кибербезопасности. Это в том числе выражается в выделении дополнительных ресурсов дипломатической службе для усиления вклада страны в многостороннее сотрудничество в области кибербезопасности по линии Европейского союза, НАТО и Организации Объединенных Наций, а также для развития сотрудничества на международном уровне с предприятиями высокотехнологичных отраслей, научно-академическими кругами и аналитическими центрами, а также контроля за экспортом цифровой продукции. Наконец, стратегия также включает инициативы, которые укрепят усилия страны на национальном и международном уровнях по созданию активной киберзащиты и усилению сдерживания.

В дополнение к инициативам, выдвинутым в рамках национальных стратегий кибербезопасности и информационной безопасности, Дания в сотрудничестве со своими партнерами и союзниками по НАТО и Европейскому союзу продолжает участвовать в широком спектре мероприятий по противодействию гибридным угрозам, таким как кибератаки и операции влияния. Дания также вносит свой вклад в дипломатические усилия по линии Организации Объединенных Наций, Европейского союза, НАТО и ОБСЕ, направленные на содействие планомерному построению свободного, открытого, стабильного, мирного и безопасного киберпространства.

В частности, Дания поддерживает идею разработки программы действий Организации Объединенных Наций, которая могла бы стать платформой для дальнейшего сотрудничества государств и негосударственных сторон, например, в плане осуществления мероприятий по наращиванию потенциала, адаптированных к их потребностям, или поддержки в рамках Организации Объединенных Наций их усилий по выполнению соответствующих мер на национальном уровне, что в свою очередь приведет к повышению коллективных устойчивости и стабильности в сфере ИКТ.

Кроме того, Дания также является активным членом Группы сотрудничества в области сетевых и информационных систем и сети групп реагирования на инциденты в области кибербезопасности, а также членом совета Агентства Европейского союза по кибербезопасности.

Содержание концепций, упомянутых в докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности

Существующие и возникающие угрозы

Дания признает, что киберпространство открывает огромные возможности для повышения благосостояния, ускорения устойчивого экономического роста и улучшения качества жизни наших граждан. Вместе с тем наша зависимость от цифровых решений создает определенные проблемы и уязвимости.

Дания обеспокоена расширением масштабов злонамеренной активности, осуществляемой государственными и негосударственными субъектами с использованием киберсредств, а также увеличением числа случаев хищения интеллектуальной собственности, совершенного с использованием кибертехнологий. Такие действия угрожают экономическому росту и стабильности международного сообщества.

Государственные и негосударственные субъекты продемонстрировали свою готовность использовать любую возможность для проведения злонамеренной активности с использованием киберсредств. Это включает в себя вмешательство в работу критически важной инфраструктуры и кражу интеллектуальной собственности с использованием киберсредств. Любые попытки помешать функционированию критически важной инфраструктуры неприемлемы и могут поставить под угрозу жизни людей. Дания особенно встревожена участившимися в последнее время случаями посягательства на безопасность и неприкосновенность продуктов и услуг ИКТ, так как это может повлечь за собой последствия на системном уровне. В частности, использование Россией кибератак на объекты критически важной инфраструктуры в ходе неспровоцированного и незаконного вторжения на Украину является абсолютно неприемлемым и поэтому должно быть решительно осуждено всем международным сообществом. Государства должны воздерживаться от совершения кибератак, проявлять должную осмотрительность и принимать оперативные и решительные меры для пресечения злонамеренной деятельности в сфере ИКТ, осуществляемой с их территории, в соответствии с международным правом и консенсусными докладами групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы и докладом Рабочей группы за 2021 год.

Как признается в предыдущих докладах Группы правительственных экспертов и в докладе Рабочей группы открытого состава, ввиду уникальных характеристик ИКТ необходимо сохранять технологическую нейтральность подхода Организации Объединенных Наций и государств-членов к борьбе с киберугрозами в контексте международной безопасности. Это соответствует признанной Организацией Объединенных Наций концепции, согласно которой существующее международное право применимо к новым областям, в том числе к сфере новейших технологий.

Как международное право применяется к использованию информационно-коммуникационных технологий

Дания решительно поддерживает многостороннюю систему, действующую на базе международного порядка, основанного на правилах, и предназначенную для борьбы с существующими и потенциальными угрозами, которые возникают в результате злонамеренного использования ИКТ.

Как признано в консенсусных докладах групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы, а также в принципах, определенных в пунктах 71 b)–g) доклада Рабочей группы за 2021 год, международное сообщество недвусмысленно заявило о том, что вопросы киберпространства в полной мере подпадают под существующие нормы международного права. Дания подчеркивает, что к поведению государств в киберпространстве применяется существующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека. В этой связи мы призываем все государства-члены действовать в соответствии со своими обязательствами.

Суверенитет, невмешательство и запрет на применение силы — это основополагающие принципы международного права, и их нарушение государствами может представлять собой международно-противоправное деяние, в ответ на которое государства могут принимать контрмеры и добиваться возмещения в соответствии с нормами об ответственности государств. Что касается понимания и толкования этих основополагающих принципов, то предстоит еще немало сделать для достижения консенсуса по данному вопросу и выработки единого подхода к нему. Дания поддерживает направленную на достижение этой

цели деятельность, которая осуществляется по линии Группы правительственных экспертов и Рабочей группы, а также других международных и региональных инициатив, таких как программа действий по поддержке ответственного поведения государств в киберпространстве.

Важно отметить, что принцип суверенитета не должен использоваться государствами для ограничения или нарушения международного права прав человека в пределах их границ. Право прав человека применимо как в Интернете, так и в реальной жизни и влечет за собой одновременно пассивное обязательство государств воздерживаться от действий, нарушающих права человека, и активную обязанность обеспечивать людям возможность пользоваться их правами и свободами.

Как указано в «Военном руководстве Дании», с точки зрения применимости международного права проведение операций в киберпространстве не отличается от использования обычного военного потенциала. Этот вопрос также отражен в национальном документе 2019 года «Совместная доктрина военных операций в киберпространстве», в соответствии с которым военное руководство обязано учитывать соображения о соблюдении норм международного права при проведении операций в киберпространстве. Таким образом, международное гуманитарное право, включая принципы предосторожности, гуманности, военной необходимости, соразмерности и избирательности, во время вооруженных конфликтов применяется к поведению государств в киберпространстве и носит исключительно защитный характер, устанавливая четкие границы своей законности. Вслед за Европейским союзом Дания хотела бы подчеркнуть, что международное право призвано служить не источником конфликтов, а инструментом для защиты гражданских лиц и ограничения несоразмерных последствий.

Рамки ответственного поведения государств в киберпространстве составлены на основе существующих норм международного права, дополняемых 11 добровольными, не имеющими обязательной силы нормами ответственного поведения, сформулированными в докладе Группы правительственных экспертов 2015 года. Дания призывает все государства придерживаться этих рамок и выполнять включенные в них рекомендации.

Ввиду того, что существующее международное право применимо к киберпространству, Дания не призывает разрабатывать новые международно-правовые инструменты в области кибербезопасности и не считает это необходимым. Вместе с тем следует более тщательно проработать единую позицию в отношении того, как существующие нормы международного права применяются к таким вопросам. Дания надеется, что работа и рекомендации Рабочей группы будут содействовать достижению большей ясности в этом вопросе и тем самым помогут государствам соблюдать свои обязательства, а также будут способствовать повышению предсказуемости и снижению риска эскалации. С этой целью в настоящее время Дания вырабатывает национальную позицию относительно того, как международное право применяется к действиям государств в киберпространстве.

Нормы, правила и принципы ответственного поведения государств

Вслед за Европейским союзом и его государствами-членами Дания призывает все государства учитывать и развивать наработки, многократно одобренные Генеральной Ассамблеей, в частности в ее резолюции 76/19, и применять согласованные нормы ответственного поведения государств, а также принимать меры укрепления доверия, которые играют важную роль в предотвращении конфликтов. Мы приветствуем инклюзивный и конструктивный диалог в рамках Рабочей

группы, а также возможность практического сотрудничества в рамках потенциальной программы действий Организации Объединенных Наций.

Огромное значение имеют дополняющие существующее международное право и проистекающие из него нормы, правила и принципы ответственного поведения государств, которые были сформулированы в поочередно принятых докладах Группы правительственных экспертов 2010, 2013, 2015 и 2021 годов и в докладе Рабочей группы. Дания будет и впредь руководствоваться международным правом, а также соблюдать эти добровольные нормы, правила и принципы. Дальнейшее выполнение этих норм должно обеспечиваться на основе расширения сотрудничества и повышения прозрачности в отношении передовой практики.

Меры укрепления доверия

Решающее значение для обмена информацией, укрепления доверия и предотвращения конфликтов имеет создание эффективных механизмов межгосударственного сотрудничества по вопросам обеспечения кибербезопасности. Региональные форумы, такие как ОБСЕ, уже создали соответствующие платформы по мерам укрепления доверия и сотрудничеству между сторонами, имеющими общие проблемы и интересы, в целях выработки эффективных с региональной точки зрения решений. Кроме того, деятельность самой Рабочей группы также следует считать мерой укрепления доверия, поскольку Рабочая группа представляет собой международный форум, на котором все государства-члены могут обмениваться информацией и делиться мнениями по вопросам, связанным с обеспечением кибербезопасности.

Дания вслед за Европейским союзом и его государствами-членами призывает международное сообщество продолжить разработку и выполнение мер укрепления доверия в киберпространстве, тем самым повышая предсказуемость поведения государств и снижая риск неправильного толкования, эскалации и конфликта, что в свою очередь способствует долгосрочной стабильности в киберпространстве.

Международное сотрудничество и помощь в деле обеспечения безопасности информационно-коммуникационных технологий и укрепления потенциала в этой сфере

Решающее значение для уменьшения рисков, возникающих в результате злонамеренного использования ИКТ, снижения напряженности и предотвращения конфликтов имеет укрепление потенциала противодействия киберугрозам наших обществ. Поэтому, как указано выше, правительство Дании внедрило целый ряд инициатив по укреплению национального потенциала противодействия киберугрозам. Аналогичным образом, Европейский союз и его государства-члены, включая Данию, также ведут совместную работу в целях укрепления потенциала противодействия во всем Европейском союзе, в частности с помощью директив по безопасности сетевых и информационных систем.

В дополнение к этим усилиям Дания — совместно с Европейским союзом и его государствами-членами — также вносит свой вклад в повышение потенциала противодействия киберугрозам развивающихся стран посредством ряда специализированных программ и инициатив, направленных на развитие навыков и потенциала в области реагирования на инциденты в области кибербезопасности, а также на содействие обмену передовым опытом.

Вслед за Европейским союзом и его государствами-членами Дания признает, что повышение потенциала противодействия цифровой инфраструктуры будет способствовать созданию более безопасного и стабильного киберпространства, и призывает все заинтересованные стороны участвовать в работе по наращиванию потенциала в этой сфере и далее призывать к более тесному сотрудничеству с ключевыми международными партнерами и организациями в поддержку наращивания потенциала в третьих странах.

Кроме того, Дания также поддерживает создание механизма Организации Объединенных Наций для содействия реализации таких программ по наращиванию потенциала с учетом потребностей, определенных государствами-бенефициарами, как программа действий, и определения механизмов, способствующих вовлечению всех заинтересованных сторон в реализацию рамок ответственного поведения.

Египет

[Подлинный текст на арабском языке]
[31 мая 2022 года]

Мнения и предложения Египта относительно укрепления информационной безопасности и содействия международному сотрудничеству в этой области

I. Национальные усилия

- В последние годы Египет активизировал свои усилия по наращиванию потенциала и разработал нормативно-правовую базу в области информационно-коммуникационной безопасности в соответствии с рекомендациями, которые содержатся в заключительных докладах Рабочей группы открытого состава и докладах Группы правительственных экспертов.
- Государственные власти Египта проводят сбалансированную политику, направленную на отслеживание киберпреступности и борьбу с ней, а также на противодействие незаконной деятельности в Интернете и социальных сетях в соответствии с законодательной базой, которая основана на ряде недавно созданных законов, включая: закон № 175 (2018) о борьбе с преступлениями в сфере информационных технологий, закон № 180 (2018) о регулировании прессы и СМИ и закон № 151 (2020) о защите персональных данных.
- Был создан Высший совет по кибербезопасности — компетентный орган и ведущий национальный центр по вопросам кибербезопасности. В рамках программы «Концепция развития Египта на период до 2030 года» начала действовать национальная стратегия кибербезопасности. Она позволит создать национальную интегрированную систему, основанную на передовом международном опыте. Она позволит также создать национальные партнерства по кибербезопасности между государственными учреждениями и частным сектором и укрепить программы киберзащиты путем создания в различных государственных секторах и повышения эффективности групп и сетей реагирования на компьютерные инциденты. Кроме того, эта стратегия направлена на создание и развитие программ повышения осведомленности в области кибербезопасности, ориентированных на определенные социально-демографические группы, например школьников, работников государственных учреждений и пожилых людей, а также на оказание поддержки научным исследованиям и инновациям в области кибербезопасности.

- Был принят ряд национальных стратегий, механизмов управления, нормативных документов и стандартов. Они охватывают базовые механизмы обеспечения кибербезопасности, механизмы контроля систем кибербезопасности и постоянный мониторинг кибербезопасности на национальном уровне.
- Египет работает над развитием двустороннего и многостороннего международного сотрудничества в области информационной безопасности и наращивания потенциала.
- Было запущено немало национальных программ и инициатив, направленных на повышение осведомленности общества, предотвращение киберрисков и уменьшение их последствий путем выпуска предупреждений о новейших и наиболее опасных слабых местах в киберзащите.
- В целях наращивания потенциала и создания квалифицированного кадрового резерва в области кибербезопасности и информационной безопасности ведется совместная работа с национальными органами и научными кругами.

II. Предложения

- Крайне важно укреплять международное сотрудничество в области кибербезопасности, чтобы свести к минимуму трансграничную преступную активность с использованием киберсредств и предотвратить совершение преступлений с использованием киберсредств. Для того чтобы государства могли противостоять незаконному использованию Интернета, нам необходимо обмениваться опытом и современными технологиями для преследования в судебном порядке всех случаев такого незаконного использования. Следует проводить учебные курсы для развития потенциала органов безопасности, которым поручена борьба с киберпреступностью.
- Необходимо принять меры по регулированию обращения криптовалют, чтобы они не использовались для финансирования незаконной деятельности. Следует также рассмотреть вопрос о создании специализированного подразделения по киберпреступности в Международной организации уголовной полиции (Интерпол) для облегчения обмена информацией между силовыми структурами, участвующими в борьбе с такой деятельностью.

Российская Федерация

[Подлинный текст на русском языке]
[31 мая 2022 года]

Двадцать первый век — время прорывного развития информационных технологий. Они завоевывают буквально все сферы жизни. Кардинальную трансформацию проходят традиционные сферы деятельности государства, общества, бизнеса. Создаются новые возможности для развития экономики и рынка труда, для повышения качества жизни людей. Вместе с тем новые технологические решения порождают и новые вызовы.

Глобальное цифровое пространство нередко становится площадкой для жесткого информационного противоборства, проведения компьютерных атак, в том числе на критическую информационную инфраструктуру, нечестной конкуренции и злоупотреблений со стороны частных компаний. Ключевые угрозы — использование информационно-коммуникационных технологий (ИКТ) в военно-политических и иных сферах в целях подрыва суверенитета, нарушение территориальной целостности, вмешательство во внутренние дела государств;

распространение вредоносного программного обеспечения в открытых источниках; применение ИКТ в террористических, экстремистских и преступных целях. Все это качественно меняет ситуацию в мире, создает повышенные риски для международной безопасности.

Россия одной из первых призвала мировое сообщество к объединению усилий в этой новой области. В 1998 году по нашей инициативе принята резолюция Генеральной Ассамблеи Организации Объединенных Наций «Достижения в сфере информатизации и телекоммуникации в контексте международной безопасности». Это был призыв к самому широкому сотрудничеству в борьбе с общими угрозами в информационной сфере, прежде всего с попытками использования новейших технологий в ущерб международному миру и стабильности. Благодаря нашим усилиям тематика информационной безопасности вошла в повестку дня Генеральной Ассамблеи Организации Объединенных Наций, принятие соответствующей резолюции по международной информационной безопасности стало ежегодным.

В 2004 году также по инициативе России в системе Организации Объединенных Наций впервые учреждена специализированная площадка для обсуждения вопросов обеспечения безопасности ИКТ — группа правительственных экспертов. Всего было созвано шесть групп правительственных экспертов. Стремительные изменения в информпространстве создали условия для вывода дискуссий на качественно новый уровень.

В 2018 году большинство стран — членов Организации Объединенных Наций одобрили предложенную Россией резолюцию о международной информационной безопасности. Документ закрепил первоначальный перечень правил, норм и принципов ответственного поведения государств в сфере использования ИКТ. Постановил перевести работу по его дальнейшему расширению и в целом дискуссию по международной информационной безопасности на более демократичную основу — в формат рабочей группы Организации Объединенных Наций открытого состава. Группа успешно завершила свою деятельность и приняла консенсусом всех государств — членов Организации Объединенных Наций итоговый доклад (Нью-Йорк, 12 марта 2021 года).

Усилиями России и единомышленников удалось обеспечить преемственность и непрерывность переговорного процесса под эгидой Организации Объединенных Наций путем создания новой Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы). Ее мандат предусматривает дальнейшую выработку правил, норм и принципов ответственного поведения государств и путей их реализации. Прежде всего — через достижение общего понимания по угрозам в сфере информационной безопасности, применимости международного права к использованию ИКТ государствами, мерам укрепления доверия и наращивания потенциала, укреплению связей между компетентными ведомствами. Механизм рабочей группы открытого состава обеспечивает лидирующую роль государств в дискуссии, дает возможность для участия в ней неправительственным субъектам.

Российские подходы к обеспечению международной информационной безопасности прозрачны и неизменны. В Стратегии национальной безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 2 июля 2021 года № 400) данная сфера обозначена как стратегический национальный приоритет. В соответствии с Основами государственной политики Российской Федерации в области международной информационной безопасности (утверждены Указом Президента Российской Федерации от 12 апреля 2021 года № 213) цель государственной политики — содействие установлению

международно-правового режима регулирования глобального информационного пространства.

Считаем необходимым заключить универсальные юридически обязывающие договоренности, направленные на предупреждение конфликтов и выстраивание взаимовыгодного сотрудничества в информационном пространстве. Основой для таких инструментов могут служить российский проект конвенции о противодействии использованию ИКТ в преступных целях, внесенный в созданном по нашей инициативе профильном Спецкомитете, а также российская концепция конвенции Организации Объединенных Наций об обеспечении международной информационной безопасности.

ИКТ должны служить задачам устойчивого развития, создания благоприятных условий для научного поиска и быстрого внедрения передовых технологических решений. Под реализацию данных установок в рамках будущих согласованных универсальных и справедливых юридических обязательств по инициативе Российской Федерации и Соединенных Штатов Америки в 2021 году принята резолюция Генеральной Ассамблеи 76/19, утвержденная консенсусом при соавторстве 108 государств — членов Организации.

Россия выступает за незыблемость цифрового суверенитета государств. Каждая страна может и должна самостоятельно определять параметры регулирования собственного информационного пространства и соответствующей инфраструктуры. Отстаиваем интернационализацию управления интернетом и равные права государств в этом процессе. Считаем неприемлемыми любые попытки ограничить их суверенное право на регулирование и обеспечение безопасности национальных сегментов глобальной сети.

Также считаем важным предпринимать правовые меры против доминирования отдельных государств в цифровой сфере как на национальном, так и на международном уровне. Важно обеспечить создание условий, при которых будут надежно и в равной степени защищены права всех пользователей в информационном пространстве. Ни одно государство или группа стран не могут единолично устанавливать принципы, правила и стандарты функционирования сети Интернет. Для решения этих задач Россия настаивает на передаче прерогатив по управлению интернетом в специализированное агентство Организации Объединенных Наций в области электросвязи и ИКТ — Международный союз электросвязи, имеющий необходимую экспертизу в этих вопросах.

Россия, как и прежде, открыта для диалога и конструктивного взаимодействия со всеми партнерами как в двустороннем формате, так и на площадках международных структур и форумов, прежде всего, в Организации Объединенных Наций.

Сингапур

[Подлинный текст на английском языке]
[31 мая 2022 года]

Сингапур твердо привержен идее укрепления основанного на правилах международного порядка в киберпространстве — порядка, который станет фундаментом для формирования доверительных отношений между государствами-членами и будет способствовать экономическому и социальному прогрессу. Чтобы в полной мере воспользоваться преимуществами цифровых технологий, международное сообщество должно создать развивать безопасное, надежное, открытое и функционально совместимое взаимосвязанное киберпространство, действующее на основе применимых норм международного права, четко

определенных стандартов норм ответственного поведения государств, эффективных мер укрепления доверия и скоординированных усилий по наращиванию потенциала. Сингапур считает крайне важным продолжать обсуждение таких вопросов, в том числе законов, правил и норм, касающихся ответственного поведения государств, в рамках Организации Объединенных Наций — единственного универсального, инклюзивного и многостороннего форума, где все государства имеют равное право голоса.

Сингапур участвовал в работе Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности в период 2019–2021 годов и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, учрежденной в соответствии с резолюцией 73/27 Генеральной Ассамблеи. Мы активно участвуем в работе ориентированной на действия результат Рабочей группы открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы) и поддерживаем усилия Председателя по организации такой работы в целях достижения прогресса в ходе обсуждения международных норм в киберпространстве и согласованных свода норм рамок ответственного поведения государств в киберпространстве. Мы по-прежнему готовы вносить конструктивный вклад в деятельность Рабочей группы в целях дальнейшего укрепления международного сотрудничества и достижению прогресса в обеспечении ответственного поведения государств в киберпространстве. В качестве сопредседателя Группы друзей по вопросам электронного управления и кибербезопасности (совместно с Эстонией) Сингапур будет продолжать использовать эту платформу для повышения осведомленности о проблемах, возникающих в киберпространстве, а также для обмена примерами передовой практики и содействия наращиванию потенциала в Организации Объединенных Наций.

Правила, нормы и принципы ответственного поведения государств

Сингапур считает, что необходимы дополнительные усилия по содействию повышению осведомленности о существующих добровольных, не имеющих обязательной силы нормах ответственного поведения государств и поддержке их соблюдения. Кроме того, Сингапур поддерживает дальнейшую выработку этих норм по мере необходимости. Например, можно было бы рассматривать в качестве особой категории критически важной инфраструктуры критически важную трансграничную информационную инфраструктуру, которая обеспечивает оказание услуг на территории нескольких государств и за защиту которой несут ответственность все государства-члены; защита этой категории должна быть включена в существующий перечень норм, поскольку угрозы в сфере ИКТ для объектов такой инфраструктуры могут оказать дестабилизирующее воздействие как на региональном, так и на глобальном уровнях[3].

Важную роль в поддержке имплементации существующей нормативной базы могут играть региональные организации. Ассоциация государств Юго-Восточной Азии (АСЕАН) приняла принципиальное решение присоединиться к 11 добровольным, не имеющим обязательной силы нормам ответственного поведения государств в сфере использования ИКТ, и на сегодняшний день остается единственной региональной организацией, принявшей эти нормы. На шестой Конференции на уровне министров стран — членов АСЕАН по вопросам

[3] Критически важная трансграничная информационная инфраструктура — это критически важная информационная инфраструктура, объекты которой принадлежат частным компаниям, эксплуатируются на трансграничной основе и не находятся при этом под юрисдикцией какого-либо одного государства.

кибербезопасности, состоявшейся в 2021 году, участники обсудили ход осуществления долгосрочного регионального плана действий стран — членов АСЕАН по имплементации норм ответственного поведения государств в киберпространстве, который направлен на обеспечение эффективной имплементации этих норм на практике, в том числе в таких областях, как сотрудничество между группами реагирования на компьютерные инциденты, защита критически важной информационной инфраструктуры и оказание взаимной помощи в вопросах кибербезопасности. В ноябре 2021 года на втором Координационном комитете АСЕАН по кибербезопасности был одобрен региональный план действий, который остается обновляемым документом для дальнейшего рассмотрения. На смену стратегии сотрудничества АСЕАН в области кибербезопасности пришла стратегия сотрудничества АСЕАН в области кибербезопасности на период 2021–2025 годов, призванная создать более безопасное и надежное киберпространство в регионе АСЕАН. Страны — члены АСЕАН договорились о создании региональной группы реагирования на компьютерные инциденты, которая будет содержать механизм обмена информацией между такими группами стран — членов АСЕАН, для усиления реагирования укрепления возможности Ассоциации реагировать на инциденты в области кибербезопасности. Был создан справочник координаторов по вопросам безопасности и использования ИКТ Регионального форума АСЕАН по вопросам безопасности в сфере использования ИКТ и самих ИКТ, с тем чтобы члены Форума могли связываться со своими коллегами в случае инцидента в области кибербезопасности.

Наращивание потенциала

Сингапур считает, что одним из основных элементов согласованной нормативной базы является наращивание потенциала, поскольку важно обеспечить, чтобы все государства обладали потенциалом для реализации нормативной базы и своих обязательств по международному праву. В соответствии с этим Сингапур стремится делиться своим опытом и знаниями на региональном и глобальном уровнях с другими государствами — членами Организации Объединенных Наций, особенно с малыми развивающимися странами.

Для поддержки наращивания потенциала на региональном (АСЕАН) уровне в 2016 году Сингапур учредил Программу укрепления киберпотенциала АСЕАН, посредством реализации которой он надеется внести вклад в наращивание потенциала стран АСЕАН в области разработки политики и стратегий, касающихся киберпространства, и решения соответствующих оперативных и технических вопросов. После положительных отзывов международных партнеров и участников о программе Сингапур объявил о создании в октябре 2019 года Центра передового опыта АСЕАН — Сингапур в области кибербезопасности с обязательством выделить в течение пяти лет (до 2023 года) 30 млн долл. США на проведение программ обучения по кибербезопасности для высокопоставленных должностных лиц АСЕАН, занимающихся политическими и техническими вопросами. Официальное открытие комплекса Центра состоялось в октябре 2021 года во время Сингапурской международной кибернедели. На сегодняшний день на счету Центра — более 30 программ, в которых приняли участие более 1250 высокопоставленных должностных лиц из стран АСЕАН и других регионов, и сотрудничество с более чем 40 партнерами — представителями правительств, частного сектора, научных кругов и неправительственных организаций. Несмотря на ограничения на поездки, вызванные пандемией коронавирусного заболевания (COVID-19), Центр продолжал проводить учебные программы в режиме онлайн и с мая 2020 года организовал 21 виртуальную программу по наращиванию потенциала.

На глобальном уровне Сингапур в партнерстве с Управлением по вопросам разоружения работает над следующими инициативами:

a) в рамках Программы Организации Объединенных Наций и Сингапура в области кибертехнологий Сингапур в партнерстве с Управлением по вопросам разоружения организует серию семинаров в различных регионах в целях разработки контрольного перечня мер по имплементации норм. Этот контрольный перечень будет оформлен в виде руководства с указанием набора действий, которые развивающиеся страны могут предпринять для имплементации 11 добровольных, не имеющих обязательной силы норм ответственного поведения государств. В марте 2022 года Сингапур провел первый семинар по имплементации норм для разработки контрольного перечня с государствами — членами АСЕАН; этот семинар был посвящен имплементации норм по защите критически важной инфраструктуры, информированию об уязвимостях и защите групп реагирования на компьютерные инциденты и групп реагирования на инциденты в области кибербезопасности;

b) в конце 2022 года Управление по вопросам разоружения и Сингапур планируют начать осуществление совместной стипендиальной программы Организации Объединенных Наций и Сингапура по кибербезопасности, призванной обучить высокопоставленных правительственных должностных лиц государств — членов Организации Объединенных Наций междисциплинарным навыкам, необходимым для эффективного контроля за национальной политикой, стратегией и деятельностью в области кибербезопасности и цифровой безопасности.

Меры укрепления доверия

Сингапур также считает, что международному сообществу следует предпринимать дальнейшие усилия по разработке мер укрепления доверия в поддержку согласованной нормативной базы, учитывая, что такие меры способны снизить риск возникновения недопонимания, а также предотвратить конфликты в киберпространстве и добиться их деэскалации. В этой связи Сингапур поддерживает создание глобального справочника национальных координаторов на оперативном или техническом уровне, в соответствии с рекомендацией Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Во второй половине 2022 года Сингапур также проведет в партнерстве с Институтом Организации Объединенных Наций по исследованию проблем разоружения (ЮНИДИР) первые занятия из цикла штабных учений для национальных координаторов по кибервопросам. Эти учения: a) предоставят возможность всем государствам — членам Организации Объединенных Наций принять участие в содержательных киберучениях независимо от текущего технического потенциала и/или статуса принадлежности к региональной организации; b) расширить возможности национальных координаторов по кибервопросам в деле реагирования на реальные инциденты и киберкризисы; и c) продемонстрировать эффективность и ценность предлагаемого глобального справочника координаторов. Такие учения ранее организовывались на региональном уровне с участием групп реагирования на компьютерные инциденты, но не были открыты для всех заинтересованных государств — членов Организации Объединенных Наций, особенно для тех, которые не входят в созданные региональные сети групп реагирования на компьютерные инциденты. Теперь ситуация изменилась: программа теоретических учений Сингапура станет первой учебной программой, открытой для всех государств-членов.

Усилия на национальном уровне

На национальном уровне Сингапур продолжает укреплять безопасность своих информационных систем и сетей по трем направлениям: создание устойчивой к внешним воздействиям инфраструктуры, укрепление безопасности киберпространства и развитие динамичной экосистемы кибербезопасности.

Создание инфраструктуры, устойчивой к внешним воздействиям

Организации, владеющие и управляющие нашей основной цифровой инфраструктурой, должны соблюдать правила и нормы кибербезопасности, в которых подробно описываются принципы кибергигиены, которым должны следовать такие организации, в частности своевременное обновление версий систем и программного обеспечения, хранение резервных копий ключевых данных и оперативное обнаружение кибервзломов. Для борьбы с развивающимися угрозами (такими как вирусы-вымогатели) в дополнение к нормам и правилам по мере необходимости также выпускаются предупреждения и рекомендации. Кроме того, в рамках усилий Сингапура по повышению безопасности и потенциала противодействия его критически важной информационной инфраструктуры, обеспечивающей оказание основных услуг, в 2019 году Агентство кибербезопасности Сингапура приступило к выполнению Генерального плана обеспечения кибербезопасности в сфере операционных технологий. В Генеральном плане, разработанном с целью улучшить межсекторальное реагирование на киберугрозы, возникающие в сфере операционных технологий, и укрепить партнерские отношения с промышленными кругами и другими заинтересованными сторонами, изложена информация об основных инициативах, касающихся людских ресурсов, процессов и технологий, призванная укрепить потенциал владельцев объектов критически важной информационной инфраструктуры и организаций, эксплуатирующих операционно-технологические системы. Агентство также разработало систему базовых требований к профессиональным качествам в области операционных технологий, которую предприятия могут использовать при создании процессов, структур или рабочих мест в сфере управления кибербезопасностью операционных технологий в своих организациях. В 2022 году Агентство введет в действие программу регулирования цепочек поставки в области критически важной информационной инфраструктуры, предусматривающую участие заинтересованных сторон, таких как правительственные учреждения, владельцы объектов критически важной информационной инфраструктуры и их поставщики. В рамках этой программы всем заинтересованным сторонам будут предоставляться рекомендации по налаживанию процессов и внедрению рациональных методов управления киберрисками, угрожающими цепочкам поставки.

Повышение безопасности киберпространства

В рамках наших усилий по повышению уровня национальной кибербезопасности в 2020 году Агентство кибербезопасности приступило к выполнению Генерального плана «Повышение безопасности киберпространства», призванного: a) обеспечить защиту ключевых объектов цифровой инфраструктуры Сингапура; b) обезопасить деятельность в киберпространстве; и c) расширить права и возможности нашего технологически подкованного населения. В Генеральном плане изложены 11 инициатив, направленных на обеспечение более систематического учета предприятиями и организациями факторов безопасности при проектировании и разработке программ и услуг, а также на повышение уровня осведомленности конечных пользователей об общих принципах кибербезопасности и правилах кибергигиены. В обеспечении безопасности нашей деятельности в киберпространстве в целом в том или ином качестве участвуют все предприятия

и организации. Для содействия этому Агентство запустило ряд программ по повышению осведомленности заинтересованных сторон о кибербезопасности, таких как пособия по кибербезопасности, предназначенные для различных заинтересованных предприятий. Это дополняется сертификацией по кибербезопасности предприятий в форме маркировки знаками “Cyber Trust” и “Cyber Essentials”, отмечающими предприятия с комплексными мерами и нормами кибербезопасности.

Агентство кибербезопасности выпускает информационные бюллетени, призванные помочь предприятиям и широкой общественности ориентироваться в уязвимостях и угрозах с использованием киберсредств и принимать соответствующие меры при их возникновении. Так, Агентство выпустило информационный бюллетень по недавней уязвимости Log4Shell и совместно с торговыми ассоциациями и палатами проинформировало сингапурских предприятий о том, как устранить уязвимость и защитить свои системы. Кроме того, у Агентства есть постоянные рекомендации, касающиеся киберпреступности, например рекомендация для населения, в которой жертвам не рекомендуется платить выкуп лицам, стоящим за вирусами-вымогателями.

Распространение Интернета вещей сопряжено с растущими рисками кибербезопасности, учитывая его широкие возможности подключения и недостаточный учет соображений кибербезопасности. Агентство кибербезопасности использует технические стандарты для повышения уровня кибергигиены и обеспечения гарантий изделий и услуг. В 2020 году Агентство ввело систему маркировки кибербезопасности для потребительских устройств, относящихся к Интернету вещей. В настоящее время на рынке представлено более 150 маркированных продуктов. Сингапур также активно поддерживает основанные на правилах международные стандарты и является страной, уполномоченной выдавать сертификаты в соответствии с соглашением о признании сертификатов соответствия общим критериям[4]. Международные стандарты помогут повысить уровень кибергигиены, обеспечить совместными усилиями безопасность киберпространства и снизить барьеры для трансграничной торговли. Сингапур надеется совместно с партнерами-единомышленниками разработать универсальную систему маркировки для обеспечения безопасности потребительского сегмента Интернета вещей, чтобы согласовать установленные международные стандарты и требования к маркировке, а также облегчить взаимное признание таких стандартов. Это позволит минимизировать фрагментацию стандартов, устранить дублирование тестирования в разных странах, снизить затраты на соблюдение национальных норм и облегчить разработчикам доступ на рынок.

Развитие динамичной экосистемы кибербезопасности

Сингапур признает, что укрепление кибербезопасности требует создания единой экосистемы кибербезопасности и поощрения инноваций в этой отрасли. Если специализирующиеся на кибербезопасности компании хотят действовать на опережение, то, с учетом быстро меняющейся ситуации с киберугрозами, им необходимо постоянно внедрять инновации и инвестировать в новые решения. Агентство кибербезопасности поддерживает инновации в области кибербезопасности, осуществляемые промышленными предприятиями, в рамках программы «Призыв к инновациям в сфере кибербезопасности». Это помогает занимающимся кибербезопасностью компаниям разрабатывать инновационные решения для удовлетворения потребностей в кибербезопасности ключевых местных конечных пользователей (например, организаций, владеющих объектами основной цифровой инфраструктуры и эксплуатирующих их, а также

[4] URL: www.commoncriteriaportal.org.

предприятий коммерческого сектора), а также стимулирует спрос в сфере кибербезопасности страны. Вместе с этим растет потребность в формировании резерва высококвалифицированных специалистов, которые могли бы взять на себя руководство вопросами кибербезопасности в организациях. Агентство сотрудничает с правительственными учреждениями, объединениями, партнерами по отрасли и академическими кругами Сингапура, стремясь добиться увеличения численности и повышения квалификации кадров, занимающихся вопросами кибербезопасности. Инициатива «Перспективные кадры Сингапура в сфере кибербезопасности» направлена на привлечение и поддержку талантливых молодых людей, интересующихся вопросами кибербезопасности, а также на оказание профессионалам в области кибербезопасности помощи в повышении квалификации. Ожидается, что в течение трех лет в рамках этой инициативы будет охвачено не менее 20 000 человек, что позволит укрепить национальный кадровый резерв в сфере кибербезопасности.

Турция

[Подлинный текст на английском языке]
[31 мая 2022 года]

В соответствии с оценками и рекомендациями, содержащимися в докладе Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, ниже представлены мнения и оценки Турции относительно усилий, прилагаемых на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в сфере информатизации и телекоммуникаций в контексте международной безопасности, а также содержание концепций, упомянутых в соответствующих докладах.

Как подчеркивается в вышеупомянутых докладах, сегодня как никогда очевидна насущная необходимость установления и поддержания международного мира, безопасности, сотрудничества и доверия в информационно-коммуникационной (ИКТ) среде. В свете диверсификации и расширения охвата киберугроз и преступлений безопасность в сфере ИКТ стала одним из основных элементов стратегии национальной обороны и международной безопасности, особенно с учетом распространения цифровых технологий и их трансграничного характера. Поэтому государства-члены прилагают активные усилия для создания необходимой технической инфраструктуры, институционального потенциала и человеческого капитала в области национальной безопасности. В целях активного предотвращения потенциальных рисков для национальной безопасности Турции планируются и предпринимаются необходимые действия, такие как развитие технологий, связанных с кибербезопасностью и конфиденциальностью данных, решение проблем, связанных с наличием квалифицированных кадров, завершение институциональной реструктуризации, поддержание правовой инфраструктуры в актуальном состоянии и обеспечение соответствия развивающимся технологиям. Кроме того, для противодействия киберпреступности необходимо сотрудничество, особенно на международном уровне. В этой связи для наиболее эффективного обнаружения источников киберпреступлений и причастных к ней преступников необходимо далее развивать обмен знаниями и информацией и международное сотрудничество.

Турция уделяет особое внимание принятию мер по укреплению национальной кибербезопасности. Ведомством, отвечающим за разработку политики, стратегий и планов действий в области национальной кибербезопасности,

является Министерство транспорта и инфраструктуры. Под его эгидой и при его участии были опубликованы и реализованы национальная стратегия и план действий в области кибербезопасности на период 2013–2014 годов и национальная стратегия и план действий в области кибербезопасности на период 2016–2019 годов. Турция, при участии всех соответствующих заинтересованных сторон, работавших по линии профильных аналитических групп, и при координации Министерства транспорта и инфраструктуры, разработала национальную стратегию и план действий в области кибербезопасности на период 2020–2023 годов.

Национальная стратегия и план действий в области кибербезопасности на период 2020–2023 годов были опубликованы в «Официальном вестнике» от 29 декабря 2020 года и включают следующие основные стратегические цели:

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

Мониторинг и измерения, связанные с планом действий, осуществляются Министерством транспорта и инфраструктуры с учетом определенных этапов реализации, мероприятий, осуществляемых ответственными учреждениями и организациями, и критериев измерения.

В то же время с 2013 года работу по противодействию инцидентам в области кибербезопасности в стране координирует национальная группа реагирования на компьютерные инциденты Турции, входящая в состав Агентства информационно-коммуникационных технологий. Помимо выявления киберугроз и реагирования на инциденты в области кибербезопасности, в том числе до, во время и после их происшествия, данная группа отвечает за принятие превентивных мер, направленных на предотвращение и сдерживание угроз в киберпространстве.

Основными направлениями деятельности национальной группы реагирования на компьютерные инциденты, связанными с кибербезопасностью, являются:

- создание 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 компьютерные инциденты, 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 2000 групп реагирования на компьютерные инциденты учрежденческого уровня. В целях смягчения рисков в киберпространстве и борьбы с киберугрозами деятельность всех групп, которые работают ежедневно и круглосуточно, координирует национальная группа. Национальная группа осуществляет мониторинг с помощью инструментов обнаружения и профилактики и поддерживает обмен информацией с соответствующими сторонами с помощью инструментов отчетности. Она разработала платформу, с помощью которой все действующие в Турции группы реагирования на компьютерные инциденты могут обмениваться информацией, в частности передавать сигналы тревоги, предупреждения и оповещения, касающиеся безопасности, что обеспечивает эффективный и безопасный канал связи.

Национальная группа организует и поддерживает проведение учебных курсов, летних лагерей и соревнований по кибербезопасности, участвовать в которых могут представители ряда сообществ. Кроме того, она проводит для других групп реагирования на компьютерные инциденты учебные занятия по таким темам, как анализ вредоносных программ и анализ журналов регистрации событий. По состоянию на апрель 2022 года в организованных Национальной группой учебных занятиях, посвященных различным аспектам кибербезопасности, приняли участие более 5000 человек.

Национальная группа 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 или продуктов сторонних производителей и обеспечивает координацию процесса управления уязвимостями.

Кроме того, в целях наращивания резерва высококвалифицированных профильных кадров Турции в 2017 году была создана Академия БТК — учебный центр, действующий при Агентстве информационно-коммуникационных технологий, который проводит онлайновые занятия по кибербезопасности и другим смежным областям для широких кругов населения. Материалы учебных занятий доступны на официальном веб-сайте Академии (www.btkakademi.gov.tr/portal).

Помимо этого, еще несколько турецких организаций, учреждений, университетов, неправительственных организаций и структур частного сектора также проводят по всей стране семинары, конференции и учебные занятия по соответствующим темам, таким как кибербезопасность и защита объектов критически важной инфраструктуры.

К числу информационно-просветительских мероприятий Агентства информационно-коммуникационных технологий относится ежегодно проводимый День безопасного Интернета, главная цель которого — поощрять осознанное и безопасное использование Интернета. На официальном веб-портале «Безопасный Интернет» (www.guvenlinet.org.tr) в открытом доступе размещены ссылки на веб-сайт о безопасности в сети и на «горячую линию» по вопросам безопасности в Интернете, при помощи которых семьи могут получить советы и рекомендации по эффективному использованию Интернета.

Кроме того, проводятся онлайновые и очные тренинги и семинары для учащихся, учителей и родителей по осознанному и безопасному использованию Интернета. Более того, многие учащиеся были охвачены школьными визитами в рамках проекта «Грузовик безопасного Интернета», который помогает детям и молодежи по всей стране непосредственно взаимодействовать с новыми технологиями, правильно использовать технологии и Интернет, а также повышает осведомленность по этому вопросу.

Стремясь обеспечить защиту от киберугроз, Турция предпринимает шаги по противодействию повышенным рискам с точки зрения цифровой безопасности и принимает соответствующие меры во время пандемии коронавирусного заболевания (COVID-19).

Информация о вредоносных программах, фишинге и других киберугрозах, эксплуатирующих уязвимости, сложившиеся в ходе пандемии COVID-19, анализируется национальной группой реагирования на компьютерные инциденты, которая работает круглосуточно и без выходных. Она использует центры управления и контроля для выявления и блокировки вредоносных цепочек киберугроз, тем самым обеспечивая защиту критически важной инфраструктуры и граждан. Составляются соответствующие отчеты о киберугрозах, которые затем передаются соответствующим сторонам. Кроме того, был подготовлен и опубликован ряд руководств, в том числе по следующим вопросам:

- принципы обеспечения безопасности удаленных подключений;
- защита пользователей от фишинговых атак;
- поддельные приложения, связанные с COVID-19;
- принципы обеспечения безопасности при настройке и использовании программного обеспечения для видеоконференций и виртуальных совещаний.

Кроме того, вступили в силу национальные профессиональные стандарты для специалистов по кибербезопасности (уровень 5), после того как они были опубликованы в «Официальном вестнике».

Турция играет важную роль во многих организациях, занимающихся вопросами кибернетической и информационной безопасности, либо являясь одним из членов-основателей, либо содействуя их совместной работе в этой сфере. В этой связи Турция придает огромное значение обмену информацией с различными странами и организациями. Турция является членом Международного союза электросвязи, а ее национальная группа реагирования на инциденты в области кибербезопасности — членом следующих структур: Форум групп оперативного реагирования и обеспечения безопасности, организация «Доверенные инициаторы», Многонациональная программа Организации Североатлантического договора (НАТО) по обмену информацией о вредоносных программах, Альянс по кибербезопасности в интересах взаимного прогресса и группа реагирования на инциденты в области кибербезопасности Организации исламского сотрудничества. Кроме того, с ноября 2015 года Турция в качестве страны-спонсора принимает участие в работе Центра передового опыта НАТО по совместной кибербезопасности. Более того, ведется работа, связанная с двусторонним и многосторонним сотрудничеством по вопросам кибербезопасности, в том числе в формате подписания меморандумов о взаимопонимании со многими странами. Турция также поддерживает активное участие в исследовательской работе таких международных организаций, как Организация Объединенных Наций, НАТО, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Организация экономического сотрудничества и развития (ОЭСР), Группа двадцати, Организация тюркских государств, Организация экономического сотрудничества, Организация экономического сотрудничества Группы восьми развивающихся стран и Региональный центр по содействию проверке и осуществлению контроля над вооружениями — Центр по сотрудничеству в сфере безопасности, внося свой вклад в их работу.

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 необходимо принять для противодействия потенциальным киберугрозам. Начиная с 2011 года в Турции пять раз проводились учения по кибербезопасности на национальном уровне и два раза — на международном. Совсем недавно — 12 и 13 октября 2021 года — в сотрудничестве с Министерством транспорта и инфраструктуры и Агентством информационно-коммуникационных технологий были проведены национальные учения «Киберщит-2021» с участием государственных учреждений и организаций. Кроме того, 19 декабря 2019 года в Анкаре Министерство и Агентство совместно организовали международные учения «Киберщит-2019». Поддержку в проведении этих учений оказали МСЭ и Альянс по кибербезопасности в интересах взаимного прогресса. Кроме того, Турция продолжает участвовать в организации и проведении целого ряда международных учений по кибербезопасности, таких как «Сомкнутые щиты НАТО», «Киберкоалиция НАТО» и Учения НАТО по урегулированию кризисов. Наряду с другими исследовательскими мероприятиями, направленными на наращивание потенциала и разработку методических указаний, международные учения по кибербезопасности остаются важным фактором повышения уровня готовности и наращивания потенциала реагирования на инциденты в области кибербезопасности во всем мире.

Другим важным учреждением в области национальной политики в сфере ИКТ является Управление цифровой трансформации при Президенте Турции.

Одним из наиболее важных и выдающихся исследований, проведенных Управлением цифровой трансформации, является публикация 24 июля 2020 года Руководства по информационно-коммуникационной безопасности. Это руководство является основным национальным справочным документом, опубликованным по данной тематике. Оно играет важную роль в укреплении потенциала киберзащиты государственных учреждений и поставщиков услуг критически важной инфраструктуры.

Ожидается, что государственные учреждения и поставщики услуг критически важной инфраструктуры завершат свои мероприятия по обеспечению соответствия требованиям в течение срока, указанного в Руководстве, и будут проводить проверки не реже одного раза в год. Правила и процедуры проверок, которые должны проводиться учреждениями в этой связи, прописаны в Руководстве по проверке информационно-коммуникационной безопасности, которое опубликовано Управлением цифровой трансформации.

Кроме того, в Турции в сотрудничестве с заинтересованными сторонами был открыт Национальный испытательный центр объектов критически важной инфраструктуры, в котором проводятся исследования по обеспечению безопасности инфраструктуры энерго- и водоснабжения. Центр, в котором моделируются системы управления энерго- и водоснабжением, обеспечивает рабочую среду для поиска и разработки защитных и профилактических решений, связанных с безопасностью критически важной инфраструктуры, а также вклада в экосистему кибербезопасности.

В соответствии со статьями, которые Указом Президента № 48, опубликованным в «Официальном вестнике» № 30928 от 24 октября 2019 года, были включены в Указ Президента об организации работы Президента № 1, опубликованный в «Официальном вестнике» № 30474 от 10 июля 2018 года, одной из основных обязанностей Агентства цифровой трансформации является разработка проектов по повышению информационной и кибернетической безопасности.

В этом контексте были осуществлены различные проекты, связанные с информационной и кибернетической безопасностью, включая конкурс киберразведки и конкурс «ХакЗевгма: захват флага».

- Конкурс киберразведки проводится в рамках учебно-просветительской деятельности, направленной на увеличение числа лиц, осведомленных в вопросах кибербезопасности; он высоко зарекомендовал себя в этом отношении. В 2021 году в рамках месячника информирования о киберпространстве Управление цифровой трансформации провело второй конкурс киберразведки.

- Конкурс «ХакЗевгма: захват флага» был организован Управлением цифровой трансформации в рамках аэрокосмического и технологического фестиваля «Технофест-2020». «ХакЗевгма» открыт для тысяч хакеров по всему миру и призван дать им возможность продемонстрировать свои таланты. Этот конкурс подготовлен с особым упором на безопасность операционных технологических систем.

Кроме того, был запущен проект «Один миллион рабочих мест», направленный на создание квалифицированного резерва специалистов по информационным технологиям и расширение занятости путем налаживания контактов обученных специалистов с работодателями. В этот проект добавлены новые функции, которые позволяют работодателям просматривать резюме, зарегистрировавшись бесплатно и без дополнительных условий. Проект, находящийся в ведении Министерства казначейства и финансов, направлен на то, чтобы к 2023 году подготовить 1 миллион человек к трудоустройству в сфере информационных технологий, и осуществляется в контексте целей Национального технологического движения для достижения цифровой трансформации в нашей стране.

Турецкий кластер кибербезопасности — это платформа, являющаяся объектом пристального внимания и поддержки Управления цифровой трансформации и призванная наладить разработку технологий в области кибербезопасности в Турции и сделать ее страной, способной конкурировать с другими странами мира, в соответствии с задачами по созданию национальной экосистемы кибербезопасности, разработке местных и национальных продуктов кибербезопасности и расширению диапазона их использования. Мероприятия, проводимые Кластером, включают:

- создание испытательно-аналитической лаборатории, обеспечивающей инфраструктуру для тестирования и развития сектора;

- создание сертификационной лаборатории;

- создание академии кибербезопасности;

- организация национальных и международных мероприятий, таких как конференции, тренинги, семинары, дискуссии и ярмарки, а также координация заявок и поставок для проведения стажировок;

- поддержка внедрения программ среднего специального и высшего образования и аспирантуры.

В дополнение к вышеупомянутым усилиям Турецким институтом стандартов и Управлением цифровой трансформации были введены отраслевые стандарты в рамках подхода к повышению кибербезопасности среди владельцев и операторов объектов критически важной инфраструктуры. Завершены исследования, связанные со стандартами 27701, 27011, 27017, 27018, 27019, 27031, 27799, 31000 и 62443 Международной организации по

стандартизации/Международной электротехнической комиссии, и стандарты, касающиеся критически важной инфраструктуры, опубликованы Турецким институтом стандартов.

Наряду с деятельностью на национальном уровне огромное значение имеет, с учетом характера кибербезопасности, развитие международного сотрудничества. С учетом широкого диапазона распространения ИКТ, связь этих технологий с такими темами, как международный мир, стабильность и безопасность, а также основные права и свободы, постоянно развивается. Такая ситуация обуславливает необходимость усилий по использованию ИКТ в мирных целях и постоянному решению государствами вопросов международной стабильности и безопасности. Очевидно, что международное право, нормы и правила, отмеченные в докладах Группы правительственных экспертов и Рабочей группы и в соответствующих исследованиях, способствуют формированию свода норм ответственного поведения государств при использовании ИКТ в контексте международного мира и безопасности. Как отмечается в указанных докладах, свое значение в усилиях по обеспечению международной стабильности и безопасности в предстоящий период сохранят такие понятия, как развитие международного сотрудничества, уважение основных прав и свобод, защита объектов критически важной инфраструктуры и предотвращение злонамеренного использования ИКТ.

В то же время следует учитывать важность защиты государственного суверенитета в киберпространстве и необходимость разработки новых норм в дополнение к существующим. Крайне важными компонентами борьбы с киберугрозами являются укрепление сотрудничества и поддержка механизмов обмена информацией и опытом, поэтому им необходимо уделять особое внимание.

Осознавая важность соблюдения норм международного права и норм ответственного поведения государств в киберпространстве и мер укрепления доверия, а также необходимость эффективного международного сотрудничества в этой сфере, Турция предпринимает решительные шаги, необходимые для достижения этих целей.

Украина

[Подлинный текст на английском языке]
[31 мая 2022 года]

Украина уже давно является жертвой продолжающейся вооруженной агрессии России и объектом связанных с ней кибератак, в том числе против критически важной инфраструктуры Украины. Соответственно, Украина полностью разделяет обоснованную обеспокоенность, выраженную в пятом пункте преамбулы резолюции 76/19 Генеральной Ассамблеи, с оговоркой, что информационные технологии и средства не только потенциально могут быть использованы, но и уже являются инструментом, активно применяемым на практике государством-агрессором, и не только против Украины.

Неоднократно подтвержденная неспособность России соблюдать свои международные обязательства ставит под сомнение ее готовность также соблюдать положения пунктов 3 и 6 постановляющей части резолюции 76/19.

То же самое касается и всеобъемлющей международной конвенции о противодействии использованию информационно-коммуникационных технологий в преступных целях, которую предлагает разработать Москва. Это связано с тем, что если разработанные Россией положения ее проекта, создающие риск

серьезного ограничения прав и свобод граждан, не пройдут в окончательный вариант конвенции, то конвенция не будет представлять интереса для Москвы.

Такое ограничение, которое предлагается в российском проекте конвенции, неприемлемо для Украины и других демократических государств, которые являются участниками Конвенции Совета Европы о киберпреступности 2001 года, но оно устраивает авторитарные режимы, в том числе режимы России и Беларуси, которые не являются участниками Конвенции.

Несмотря на военную и кибернетическую агрессию России, Украина продолжает укреплять свою систему кибербезопасности при материальной и консультативной помощи западных партнеров.

Основными субъектами национальной системы кибербезопасности, созданной в соответствии со Стратегией кибербезопасности Украины, являются Министерство обороны, Государственная служба специальной связи и защиты информации, Служба безопасности, Национальная полиция и Национальный банк. Эта система обеспечивает взаимодействие всех государственных учреждений, местных органов самоуправления, воинских подразделений, правоохранительных органов, научно-исследовательских и образовательных учреждений, гражданских групп, предприятий и организаций, независимо от формы собственности, которые занимаются вопросами электронной коммуникации и информационной безопасности или являются владельцами объектов критически важной информационной инфраструктуры.

Субъекты обеспечения работы национальной системы кибербезопасности знакомы с оценками и рекомендациями, содержащимися в докладах Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности.

Совет национальной безопасности и обороны Украины координирует и контролирует деятельность предприятий сектора безопасности и обороны, обеспечивая кибербезопасность Украины в рамках деятельности своего рабочего органа — Национального координационного центра кибербезопасности.

Центр выполняет надзорные функции и решает задачи, связанные с анализом состояния национальной кибербезопасности и готовности к борьбе с киберугрозами, а также прогнозированием и выявлением соответствующих потенциальных и актуальных угроз.

Реализовав предыдущую Стратегию кибербезопасности Украины на период 2016–2020 годов, государство смогло сформировать ядро национальной системы кибербезопасности. Украина укрепила потенциал, позволяющий дальнейшее развитие системы на основе сдерживания, потенциала противодействия киберугрозам и взаимодействия.

Целью действующей Стратегии кибербезопасности Украины, разработанной на период 2021–2025 годов, является создание условий для безопасного функционирования киберпространства и его использования в интересах человека, общества и государства. Этот документ основан на принципах сдерживания, потенциала противодействия киберугрозам и взаимодействия.

Вышеупомянутые усилия позволили Украине выявить подготовку Россией злонамеренных кибератак на украинскую инфраструктуру, которые совпали с физической агрессией. С осени 2021 года мы наблюдали рост числа атак хакерских групп, связанных с Россией, на важных украинских поставщиков цифровых и телекоммуникационных услуг. Качество этих атак также возросло, они

стали более целенаправленными, с использованием более сложных инструментов.

Однако следует отметить, что большинство этих кибератак не были успешными. Наши заинтересованные стороны при поддержке наших международных партнеров обнаружили их и смягчили последствия.

Украина активно развивает сотрудничество в кибернетической сфере, прежде всего с Соединенными Штатами, Великобританией, Эстонией и другими западными странами-партнерами, Европейским союзом и Организацией Североатлантического договора (НАТО). Она получает финансовую помощь, а также консультации в рамках двусторонних и многонациональных учебных курсов, семинаров и конференций за рубежом и на Украине, а также помощь, современное оборудование и программное обеспечение для решения задач кибербезопасности, проведения профессиональной компьютерной экспертизы и расследования киберпреступлений.

Украина благодарна за недавнее заявление Соединенных Штатов, Великобритании, Европейского союза и других стран и институтов, в котором осуждаются агрессивные действия России в киберпространстве против Украины и других стран.

С 2016 года Министерство иностранных дел Украины организовало 22 раунда двусторонних киберконсультаций с 13 странами (Япония, Сингапур, Малайзия, Финляндия, Соединенные Штаты, Германия, Соединенное Королевство, Эстония, Нидерланды, Словения, Испания, Бразилия и Израиль). Подобные консультации с несколькими государствами были запланированы и на 2022 год, но были отложены из-за российского военного вторжения.

В области киберзащиты Украина тесно сотрудничает с целевым фондом НАТО по киберзащите для повышения технических возможностей страны в противодействии киберугрозам и надеется на эффективное сотрудничество с альянсом в качестве страны — участницы Центра передового опыта НАТО по совместной киберзащите.

Украина будет благодарна всем тем государствам — членам Организации Объединенных Наций, которые могут оказать содействие в реализации следующих проектов, осуществляемых в соответствии с текущей стратегией кибербезопасности этой страны с целью укрепления потенциала в области кибербезопасности и киберзащиты, а также развития информационно-технологической инфраструктуры и услуг сети государственных ситуационных центров:

- создание киберполигона и проведение общенациональных учений в области кибербезопасности;
- аналитические инструменты в целях выявления киберугроз для технологических платформ;
- национальный резервный центр для критически важных государственных информационных ресурсов;
- национальная система мониторинга киберугроз;
- государственная платформа облачных услуг в области кибербезопасности.

Министерство иностранных дел готово предоставить подробную информацию об этих проектах и оказать содействие в установлении контактов с их исполнителями.

Опыт Украины показывает, что для борьбы с серьезными и постоянными киберугрозами и кибератаками необходимо усилить сотрудничество на разных

уровнях — между государственными органами власти, частным сектором и международными партнерами — с тем чтобы создать необходимый потенциал и эффективно реагировать на такие угрозы.

III. Ответы, полученные от межправительственных организаций

Европейский союз

[Подлинный текст на английском языке]
[31 мая 2022 года]

Киберпространство, включая глобальный открытый Интернет, стало одной из основ нашего общества. Оно служит платформой, обеспечивающей связь и экономический рост. Европейский союз и его государства-члены поддерживают открытое, свободное, глобальное, стабильное, мирное и безопасное киберпространство на основе верховенства права, прав человека, основных свобод и демократических ценностей, которые обеспечивают социальное, экономическое и политическое развитие во всем мире.

По мере того как Интернет и информационно-коммуникационные технологии (ИКТ) становятся все более заметной частью нашей жизни, наша зависимость от этих технологий делает нас все более уязвимыми к их неправомерному использованию. Киберпространство все чаще используется в злонамеренных целях, а усиливающаяся поляризация на международном уровне препятствует эффективной реализации принципа многосторонности. Безответственное поведение России в киберпространстве является неотъемлемой частью ее незаконного и неоправданного вторжения на Украину и противоречит ожиданиям всех государств — членов Организации Объединенных Наций, включая Российскую Федерацию, в отношении согласованных норм ответственного поведения государств Организации Объединенных Наций. Кроме того, злонамеренные атаки на критически важную инфраструктуру представляют собой серьезный глобальный риск. Ограничения, налагаемые на доступ к Интернету и пользование им, активизация злонамеренной активности с использованием киберсредств, в частности деятельности, затрагивающей безопасность и целостность информационно-коммуникационных продуктов и услуг, угрожают открытому, свободному, глобальному, стабильному и безопасному киберпространству, а также демократии, верховенству права, правам человека и основным свободам.

Европейский союз и его государства-члены регулярно выражают обеспокоенность по поводу такой злонамеренной деятельности, которая подрывает основанный на правилах международный порядок и повышает риск возникновения конфликтов. Злонамеренное использование ИКТ уменьшает полезность Интернета и информационно-коммуникационных технологий для общества в целом и свидетельствует о готовности некоторых субъектов к действиям, угрожающим международной безопасности и стабильности. Все субъекты должны воздерживаться от безответственных и дестабилизирующих действий в киберпространстве.

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

Важнейшим элементом поддержания международного мира и стабильности, помогающим снизить риск возникновения конфликтов и способствующим решению связанных с цифровизацией экономики и общества проблем, является

укрепление глобального потенциала противодействия киберугрозам. Глобальный потенциал противодействия киберугрозам снижает способность потенциальных злоумышленников использовать информационно-коммуникационные технологии в неблаговидных целях и укрепляет способность государств эффективно реагировать на инциденты в области кибербезопасности и преодолевать их последствия. Европейский союз и его государства-члены решительно поддерживают вышеупомянутую концепцию открытого, свободного, глобального, стабильного и безопасного киберпространства путем продвижения и реализации всеобъемлющей и многогранной стратегии предотвращения конфликтов и обеспечения стабильности в киберпространстве, в том числе на основе двустороннего, регионального и многостороннего взаимодействия. В рамках этой стратегии Европейский союз стремится укреплять глобальный потенциал противодействия, поддерживать и стимулировать общее понимание основанного на правилах международного порядка в киберпространстве, а также разрабатывать и осуществлять меры по налаживанию практического взаимодействия, включая региональные меры по укреплению доверия.

В стратегии кибербезопасности 2013 года под названием «Открытое, безопасное и защищенное киберпространство»[5], а также в упомянутых ниже последующих программных документах, инструментах и стратегиях изложено всеобъемлющее видение Европейского союза в отношении наилучших путей предотвращения сбоев и атак в киберпространстве и реагирования на них. Они направлены на укрепление ценностей Европейского союза и формирование условий для роста цифровой экономики. Некоторые конкретные меры направлены на повышение потенциала противодействия киберугрозам информационных систем, снижение киберпреступности и укрепление международной политики Европейского союза в области кибербезопасности и киберзащиты.

В феврале 2015 года в своих заключениях по кибердипломатии[6] Совет Европейского союза подчеркнул важность дальнейшей проработки и реализации общего и всеобъемлющего подхода Европейского союза к кибердипломатии, который бы содействовал соблюдению прав человека и уважению основных ценностей Европейского союза, обеспечивал свободу выражения мнений, способствовал гендерному равенству, стимулировал экономический рост, предусматривал меры по борьбе с киберпреступностью, смягчал угрозы кибербезопасности, помогал предотвращать конфликты и обеспечивал стабильность в сфере международных отношений. Европейский союз также призывает к укреплению многосторонней модели управления Интернетом и к активизации усилий по наращиванию соответствующего потенциала в третьих странах. Кроме того, Европейский союз признает важность взаимодействия с ключевыми партнерами и международными организациями. Европейский союз подчеркивает также, что неотъемлемыми элементами общего и всеобъемлющего подхода Европейского союза к кибердипломатии являются применимость существующего международного права в киберпространстве и в области международной безопасности, актуальность норм поведения и важность управления Интернетом.

Как явствует из результатов обзора Стратегии кибербезопасности за 2013 год, Европейский союз еще больше укрепил свои структуры и потенциал в области кибербезопасности, действуя на скоординированной основе, при полном сотрудничестве своих государств-членов и различных заинтересованных

[5] См. совместное сообщение для Европейского парламента, Совета, Европейского экономического и социального комитета и Комитета регионов, озаглавленное «Стратегия кибербезопасности Европейского союза: открытое, безопасное и защищенное киберпространство».

[6] 6122/15, Council Conclusions on Cyber Diplomacy.

структур и с учетом уважения их компетенции и обязанностей. В 2017 году в совместном сообщении, озаглавленном «Потенциал противодействия, сдерживание и оборона: обеспечение надежной кибербезопасности Европейского союза»[7] были определены масштаб задач и комплекс мер, предусмотренных на уровне Европейского союза и призванных повысить его готовность к решению постоянно растущих проблем в сфере кибербезопасности.

Озабоченность постоянно усугубляющимися проблемами в сфере кибербезопасности послужила стимулом к разработке механизма совместного дипломатического реагирования Европейского союза на злонамеренную активность с использованием киберсредств — инструментария кибердипломатии[8]. Международное сообщество должно быть озабочено растущей способностью и готовностью государственных и негосударственных субъектов добиваться своих целей с помощью злонамеренной активности с использованием киберсредств. Такие действия могут являться международно-противоправными деяниями и иметь дестабилизирующие и многоуровневые последствия, сопряженные с повышенным риском возникновения конфликта. Европейский союз и его государства-члены привержены урегулированию международных споров в киберпространстве мирными средствами. В этой связи механизм совместного дипломатического реагирования Европейского союза вписывается в подход Европейского союза к кибердипломатии, направленный на предотвращение конфликтов, смягчение угроз в сфере кибербезопасности и повышение стабильности международных отношений. Этот механизм стимулирует сотрудничество, способствует смягчению непосредственных и долгосрочных угроз и оказывает влияние на поведение злоумышленников в долгосрочной перспективе. Он также обеспечивает надлежащую координацию с механизмами Европейского союза по урегулированию кризисов, включая План скоординированного реагирования на крупномасштабные инциденты и кризисы в сфере кибербезопасности. Европейский союз и его государства-члены призывают международное сообщество укреплять международное сотрудничество в интересах формирования открытого, свободного, глобального, стабильного и безопасного киберпространства, в котором в полной мере соблюдались бы права человека, основные свободы и верховенство права. Они преисполнены решимости продолжать свои усилия по предотвращению, пресечению и сдерживанию злонамеренных действий и реагированию на них и стремятся в этой связи к укреплению международного сотрудничества.

В декабре 2020 года Европейский союз более подробно изложил свою стратегию[9] кибербезопасной цифровой трансформации в условиях комплексных угроз. Стратегия кибербезопасности Европейского союза для цифрового десятилетия направлена на поощрение и защиту открытого, свободного, глобального, стабильного и безопасного киберпространства, основанного на правах человека, основных свободах, демократии и верховенстве права. Эта стратегия содержит конкретные предложения по обеспечению потенциала противодействия, предотвращению и сдерживанию киберугроз и реагированию на них, а также по развитию глобального и открытого киберпространства. Предотвращение неправомерного использования технологий, защита критически важной инфраструктуры и обеспечение целостности цепочек поставок также позволяют

[7] См. совместное сообщение для Европейского парламента и Совета, озаглавленное «Потенциал противодействия, сдерживание и оборона: обеспечение надежной кибербезопасности Европейского союза».

[8] 9916/17, Draft Council Conclusions on a Framework for a Joint European Union Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”).

[9] См. Joint Communication to the European Parliament and the Council on the European Union’s Cybersecurity Strategy for the Digital Decade and 7290/21 of 22 March 2021, Council Conclusions on the European Union’s Cybersecurity Strategy for the Digital Decade.

Европейскому союзу добиться соответствия нормам, правилам и принципам ответственного поведения государств, принятым Организацией Объединенных Наций.

Международная политика Европейского союза по вопросам киберпространства направлена на поддержание уважения основных ценностей Европейского союза, определение норм ответственного поведения и поддержку применения существующих норм международного права в киберпространстве; при этом она предусматривает оказание странам, не входящим в состав Европейского союза, помощи в наращивании потенциала в области кибербезопасности и стимулирование международного сотрудничества в регулировании и использовании киберпространства. Европейский союз продолжает работать с международными партнерами в целях расширения и поощрения открытого, свободного, глобального, стабильного и безопасного киберпространства, в котором соблюдаются нормы международного права, в частности Устава Организации Объединенных Наций, а также добровольные, не имеющие обязательной силы нормы, правила и принципы ответственного поведения государств. Очевидно, что для укрепления мира и безопасности в киберпространстве необходимо внедрить свод норм ответственного поведения государств в киберпространстве Организации Объединенных Наций, согласованный предыдущей Группой правительственных экспертов и Рабочей группой открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и одобренный Генеральной Ассамблеей. Европейский союз, совместно с 60 государствами — членами Организации Объединенных Наций, предлагает разработать программу действий по поощрению ответственного поведения государств в киберпространстве.

Такая программа действий, с опорой на существующий свод норм, единогласно одобренный Генеральной Ассамблеей, предусматривает создание постоянного, инклюзивного и прикладного механизма в рамках Организации Объединенных Наций в целях содействия выполнению консенсусных докладов и оказания поддержки государствам в осуществлении национальной политики кибербезопасности, в частности посредством разработки программ наращивания потенциала с учетом потребностей, озвученных государствами-бенефициарами. Кроме того, она обеспечит наличие в рамках Организации Объединенных Наций институционального механизма сотрудничества с другими заинтересованными сторонами, такими как частный сектор, научные круги и гражданское общество, что позволит улучшить взаимодействие с ними по вопросам, касающимся их соответствующих обязанностей по поддержанию открытой, свободной, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. Программа действий будет дополнять другие соответствующие процессы, такие как Рабочая группа открытого состава по вопросам безопасности в сфере использования ИКТ и самих ИКТ (2021–2025 годы), и действовать в координации с ними.

21 марта 2022 года, в целях укрепления своей способности прогнозировать и сдерживать существующие и быстро возникающие угрозы и вызовы и реагировать на них, а также защищать интересы безопасности Европейского союза, Европейский союз официально утвердил Стратегический компас[10]. Компас содержит амбициозный план действий Европейского союза по укреплению политики безопасности и обороны к 2030 году, включая укрепление инструментария кибердипломатии Европейского союза и дальнейшее развитие политики

[10] 7371/22, “A Strategic Compass for Security and Defence — For a European Union that protects its citizens, values and interests and contributes to international peace and security”.

кибероборонь Европейского союза для повышения эффективности готовности к кибератакам и реагирования на них.

Европейский союз и его государства-члены напоминают о принятии 23 мая 2022 года выводов Совета Европейского союза о развитии позиции Союза по вопросам, связанным с киберпространством. Эта позиция призвана продемонстрировать решимость Европейского союза обеспечить немедленное и долгосрочное реагирование на действия представляющих угрозу субъектов, стремящихся лишить Европейский союз безопасного и открытого доступа к киберпространству.

Содержание концепций, упомянутых в докладе Рабочей группы и докладах Группы правительственных экспертов

Существующие и возникающие угрозы

Европейский союз и его государства-члены признают, что киберпространство открывает широкие возможности как для экономического роста, так и для устойчивого и инклюзивного развития. Тем не менее, все еще существуют серьезные угрозы ИКТ, упомянутые в предыдущих докладах Группы правительственных экспертов[11] и в докладе Рабочей группы, которые представляют собой постоянно видоизменяющиеся проблемы.

Европейский союз и его государства-члены обеспокоены расширением масштабов вредоносной деятельности в киберпространстве, включая злонамеренное использование информационно-коммуникационных технологий как государственными, так и негосударственными субъектами, а также увеличение числа случаев хищения интеллектуальной собственности при помощи кибертехнологий. Такое поведение подрывает экономический рост, ставит под угрозу целостность, безопасность и стабильность мирового сообщества и может иметь дестабилизирующие и многоуровневые последствия, сопряженные с повышенным риском возникновения конфликта.

Пандемия коронавирусного заболевания (COVID-19) продемонстрировала риски и последствия злонамеренной деятельности в сфере ИКТ. Европейский союз и его государства-члены зафиксировали случаи киберугроз и злонамеренной активности с использованием киберсредств, направленных против оказывающих жизненно необходимые услуги, и признают уязвимость критически важной информационной инфраструктуры, базовых систем обслуживания населения, технических систем, необходимых для обеспечения общей доступности или работоспособности Интернета, а также учреждений системы здравоохранения и других организаций критически важных секторов в государствах-членах и их партнерах. Европейский союз и его государства-члены особенно обеспокоены участившимися посягательствами на безопасность и неприкосновенность информационно-коммуникационных продуктов и услуг, так как это может повлечь за собой системные последствия. Кроме того, в контексте безответственного поведения России в киберпространстве как неотъемлемой части ее незаконного и неоправданного вторжения на Украину, Европейский союз и его государства-члены наблюдали кибератаки с использованием разрушительных инструментов, таких как программы для уничтожения данных для выведения систем из строя, а также перебои в обслуживании, попытки вторжения, искажение внешнего вида веб-страницы и DDoS-атаки, направленные на Украину, с потенциальным распространением на другие страны, в частности на соседей Украины.

[11] A/75/816.

Европейский союз и его государства-члены осуждают это злонамеренное поведение в киберпространстве, включая злонамеренную деятельность в сфере ИКТ, направленную на использование уязвимостей, и подчеркивают свою неизменную поддержку усилий по укреплению глобального потенциала противодействия киберугрозам. Любые попытки привести к перебоям в работе критически важной инфраструктуры неприемлемы и могут поставить под угрозу жизни людей.

Европейский союз и его государства-члены призывают все страны не допускать сознательного использования их территорий для международно-противоправных деяний в киберпространстве с использованием ИКТ и принимать соответствующие меры против субъектов, осуществляющих такую деятельность с их территории, в соответствии с международным правом и консенсусными докладами групп правительственных экспертов за 2010, 2013, 2015 и 2021 годы и докладом Рабочей группы за 2021 год. Европейский союз и его государства-члены вновь подчеркивают, что государства должны принимать все соответствующие меры и обоснованно доступные и возможные шаги для обнаружения, расследования и урегулирования такой ситуации.

Кроме того, как признается в предыдущих докладах Группы правительственных экспертов и Рабочей группы, ввиду уникального характера, присущего информационно-коммуникационным технологиям, подход Европейского союза к борьбе с киберугрозами в контексте международной безопасности характеризуется адаптивностью к новым технологическим достижениям; при этом отмечается, что нормы ответственного поведения государств в киберпространстве являются технологически нейтральными. Это соответствует признанной Организацией Объединенных Наций концепции, согласно которой к новым областям применяются существующие нормы международного права.

Европейский союз и его государства-члены поддерживают развитие и применение лишь тех основанных на использовании ИКТ технологий, систем и услуг, которые обеспечивают полное соблюдение применимых положений и норм международного права, в частности Устава Организации Объединенных Наций, а также норм международного гуманитарного права и права прав человека.

Порядок применения норм международного права к использованию информационно-коммуникационных технологий

Европейский союз и его государства-члены решительно поддерживают эффективную многостороннюю систему, в основе которой лежит основанный на правилах международный порядок и которая способствует решению нынешних и будущих глобальных проблем в киберпространстве.

Подлинно универсальный механизм обеспечения кибербезопасности может опираться только на существующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека. Европейский союз и его государства-члены подтверждают, что к поведению государств в киберпространстве применимы нормы существующего международного права, что признается в докладах Группы правительственных экспертов за 2010, 2013, 2015 и 2021 годы, а также принципы, установленные в пунктах 71 b)–g) доклада Рабочей группы за 2021 год.

Международное право, в том числе международное гуманитарное право, которое включает принципы гуманности, избирательности, предосторожности, военной необходимости и соразмерности, применяется к поведению государств

в киберпространстве и носит исключительно защитный характер, устанавливая четкие границы своей законности, в том числе в контексте конфликтов. Европейский союз подчеркивает, что международное гуманитарное право не является фактором, способствующим возникновению конфликтов, а определяет правила, регулирующие военные операции в целях ограничения их последствий и, в частности, для защиты гражданского населения.

Кроме того, закрепленные в соответствующих международных договорах права человека и основные свободы должны уважаться и соблюдаться как в Интернете, так и в реальной жизни. Европейский союз и его государства-члены приветствуют тот факт, что значение этих принципов было подтверждено Советом по правам человека[12] и Генеральной Ассамблеей, а также Группой правительственных экспертов и Рабочей группой.

По этим причинам на данном этапе Европейский союз и его государства-члены не призывают к созданию новых международно-правовых инструментов по кибербезопасности, подчеркивая, что необходимо провести дополнительную работу, чтобы прояснить порядок применения норм международного права в отношении вопросов киберпространства.

Европейский союз и его государства-члены вновь заявляют о том, что они поддерживают продолжение диалога и сотрудничества с целью содействовать общему пониманию порядка применения существующего международного права к использованию ИКТ государствами, а также поддерживают усилия по внесению юридической ясности в вопрос о том, как применяется существующее международное право, поскольку оно будет способствовать поддержанию мира, предотвращению конфликтов и обеспечению глобальной стабильности.

Мы продолжаем поддерживать усилия по расширению применения действующего международного права в киберпространстве, в том числе по обмену соответствующей информацией и передовым опытом. Мы обязуемся и далее представлять информацию о национальных позициях в отношении принципов и порядка применения международного права к использованию ИКТ государствами, поскольку это способствует транспарентности и содействует глобальному пониманию национальных подходов, что имеет основополагающее значение для поддержания долгосрочного мира и стабильности и снижения риска возникновения конфликтов в результате действий, совершаемых в киберпространстве. Дальнейшее внимание следует уделять повышению осведомленности и наращиванию потенциала в том, что касается применимости существующего международного права в качестве средства укрепления стабильности и предотвращения конфликтов в киберпространстве.

Нормы, правила и принципы ответственного поведения государств

Европейский союз и его государства-члены призывают все государства учитывать и развивать наработки, многократно одобренные Генеральной Ассамблеей, в частности в ее резолюции 76/19, и поощрять применение этих согласованных норм и принятие мер по укреплению доверия, которые играют важную роль в предотвращении конфликтов.

При использовании ИКТ Европейский союз и его государства-члены руководствуются существующими нормами международного права, а также придерживаются добровольных норм, правил и принципов ответственного поведения государств, в частности применительно к киберпространству, как это было сформулировано в докладах Группы правительственных экспертов за 2010,

[12] См. резолюцию 20/8 Совета по правам человека.

2013, 2015 и 2021 годы. Продолжение инклюзивного и конструктивного диалога в рамках Рабочей группы _____ приветствуется в целях дальнейшего углубления обсуждения этого свода норм и проблем безопасности, связанных с использованием ИКТ. Мы считаем, что практическое продвижение вперед должно стимулировать расширение сотрудничества и повышение прозрачности для обмена передовым опытом, в том числе по вопросам порядка применения существующих норм Группы правительственных экспертов, через соответствующие инициативы и структуры, такие как региональные организации и учреждения, в целях содействия повышению осведомленности и эффективного осуществления согласованных норм ответственного поведения государств.

Меры укрепления доверия

Разработка эффективных механизмов государственного сотрудничества и взаимодействия в киберпространстве — это важнейший компонент деятельности по предотвращению конфликтов. Региональные форумы зарекомендовали себя в качестве подходящих платформ, предоставляющих сторонам с общими проблемами и интересами пространство для диалога и сотрудничества в целях выработки эффективных с региональной точки зрения решений.

Разработка и реализация мер по укреплению доверия в киберпространстве, включая меры по укреплению сотрудничества и транспарентности, в рамках Организации по безопасности и сотрудничеству в Европе, Регионального форума Ассоциации государств Юго-Восточной Азии, Организации американских государств и других региональных учреждений повысят предсказуемость поведения государств и снизят риск неправильного толкования, эскалации напряженности и возникновения конфликтов в результате инцидентов в сфере ИКТ, способствуя тем самым долгосрочной стабильности в киберпространстве.

Международное сотрудничество и помощь в деле обеспечения безопасности информационно-коммуникационных технологий и укрепления потенциала в этой сфере

В целях предотвращения конфликтов и уменьшения очагов напряженности, возникающих в результате ненадлежащего использования ИКТ, Европейский союз и его государства-члены стремятся к укреплению потенциала противодействия во всем мире, особенно в развивающихся странах, как к средству решения проблем, связанных с цифровизацией экономики и общества, и как к средству снижения способности потенциальных нарушителей неправомерно использовать ИКТ в неблаговидных целях. Потенциал противодействия укрепляет способность государств эффективно реагировать на киберугрозы и преодолевать их последствия.

Европейский союз и его государства-члены поддерживают ряд специальных программ и инициатив, направленных на оказание странам помощи в развитии навыков и потенциала в сфере борьбы с инцидентами в области кибербезопасности, а также поддерживают инициативы по обмену передовым опытом, будь то по линии прямого диалога, двусторонних контактов или взаимодействия в рамках региональных и многосторонних учреждений.

Европейский союз и его государства-члены отмечают, что содействие наращиванию надлежащего защитного потенциала и повышению безопасности цифровых продуктов, процессов и услуг будет способствовать формированию более безопасного и надежного киберпространства. Мы признаем ответственность всех соответствующих сторон за участие в работе по укреплению потенциала в этой сфере, а также призываем к более тесному сотрудничеству с ключевыми международными партнерами и организациями в поддержку наращивания

потенциала в третьих странах. Европейский союз и его государства-члены придают особое значение укреплению международной безопасности и стабильности в киберпространстве и намерены с этой целью поощрять и поддерживать конкретные действия по обеспечению ответственного поведения государств в киберпространстве и укреплять сотрудничество в области наращивания потенциала в кибернетической сфере, в частности по линии вспомогательного механизма, который будет работать под эгидой Организации Объединенных Наций и в рамках которого будут разрабатываться программы наращивания потенциала, учитывающие потребности, озвученные государствами-бенефициарами, такие как упомянутая выше программа действий, и определения механизмов, способствующих вовлечению всех заинтересованных сторон в реализацию свода норм ответственного поведения.