Организация Объединенных Наций A/76/187

Генеральная Ассамблея

Distr.: General
19 July 2021
Russian
Original: English/Spanish

Семьдесят шестая сессия
Пункт 96 предварительной повестки дня*
Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/76/150.

21-10045 (R) 130921 160921

I. Введение

1. 7 декабря 2020 года Генеральная Ассамблея приняла резолюцию 75/32, озаглавленную «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности», по пункту повестки дня «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

2. В пункте 2 этой резолюции Генеральная Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладах Группы правительственных экспертов, 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 докладах Группы правительственных экспертов.

3. Во исполнение этой просьбы 18 февраля 2021 года всем государствам-членам была направлена вербальная нота с предложением представить информацию по этому вопросу. В целях содействия представлению государствами-членами мнений по вышеизложенным вопросам крайним сроком было установлено 31 мая 2021 года.

4. Ответы, полученные на момент составления настоящего доклада, содержатся в разделах II и III ниже. Дополнительные ответы, полученные после 31 мая 2021 года, будут размещены на веб-сайте Управления по вопросам разоружения[1] на том языке, на котором они были представлены. Добавления издаваться не будут.

II. Ответы, полученные от правительств

Австралия

[Подлинный текст на английском языке]
[31 мая 2021 года]

В ответ на содержащуюся в резолюции 75/32 Генеральной Ассамблеи просьбу Австралия приветствует возможность изложить свои взгляды по вопросу о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. Настоящая информация подготовлена на основе данных, представленных Австралией в ответ на резолюции 74/28 в 2020 году, 70/237 в 2016 году, 68/243 в 2014 году и 65/41 в 2011 году и касающихся достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Стратегия международного взаимодействия в киберпространстве и по вопросам критически важных технологий

21 апреля 2021 года министр иностранных дел Австралии Марис Пейн представила Стратегию международного взаимодействия в киберпространстве и по вопросам критически важных технологий, в которой изложены интересы и задачи Австралии в киберпространстве и в связи с критически важными

[1] http://www.un.org/disarmament/ict-security.

технологиями. Главной целью Австралии является обеспечение безопасности, защищенности и процветания Австралии, Индо-Тихоокеанского региона и мира при использовании возможностей, обеспечиваемых киберпространством и критически важными технологиями (www.internationalcybertech.gov.au/).

В Стратегии определены интересы Австралии в достижении этой цели по всему спектру вопросов, касающихся киберпространства и критически важных технологий. Они включают в себя основные принципы и ценности страны — права человека, верховенство права, справедливость, открытую конкуренцию, безопасность, транспарентность, уважение и добросовестность.

В Стратегии выделены три основные составляющие — ценности, безопасность и процветание, — на которые Австралия должна ориентироваться в рамках международного взаимодействия в киберпространстве и по вопросам критически важных технологий:

a) *ценности.* Австралия всегда будет придерживаться основанного на ценностях подхода к использованию киберпространства и критически важных технологий и противостоять попыткам применения технологий с целью подорвать эти ценности;

b) *безопасность.* Австралия всегда будет поддерживать международный мир и стабильность, а также безопасность, надежность и отказоустойчивость технологий;

c) *процветание.* Австралия всегда будет выступать за то, чтобы киберпространство и технологии способствовали устойчивому экономическому росту и развитию для повышения уровня благосостояния.

6 августа 2020 года Австралия также обнародовала Стратегию обеспечения кибербезопасности 2020 года, направленную на создание более безопасного онлайн-пространства для австралийцев, их предприятий и основных служб, имеющих особое значение для Австралии (www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf).

Основа для ответственного поведения государств в киберпространстве

С учетом все большего усиления власти и влияния государств в киберпространстве Австралия находит важным наличие четких правил в этой области. В целом в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности за 2010 год (A/65/201), 2013 год (A/68/98) и 2015 год (A/70/174) 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 отмечается необходимость принимать меры по укреплению доверия и скоординированным образом наращивать потенциал. Действуя воедино, международное право, нормы, меры по укреплению доверия и наращивание потенциала обеспечивают основу для безопасности, стабильности и процветания киберпространства и часто упоминаются как рамки ответственного поведения государств.

Австралия принимала активное участие в двух завершившихся в 2021 году процессах Организации Объединенных Наций, касавшихся ответственного поведения государств в киберпространстве: в рамках шестой Группы правительственных экспертов (см. A/76/135) и Рабочей группы открытого состава (см. A/75/816), которые подтверждают эти рамки и отталкиваются от них.

Австралия подтверждает свое обязательство действовать в соответствии со сводными докладами Группы правительственных экспертов за 2010, 2013, 2015 и 2021 годы (A/65/201, A/68/98 и A/70/174) и с докладом Рабочей группы открытого состава (A/75/816).

Международное право

Позиция Австралии относительно применения международного права к поведению государств в киберпространстве представлена в ряде документов: Стратегии международного взаимодействия Австралии в киберпространстве 2017 года (www.internationalcybertech.gov.au/about/2017-International-Cyber-Engagement-Strategy), Дополнении по вопросам международного права 2019 года (https://www.internationalcybertech.gov.au/sites/default/files/2020-11/2019%20Legal%20Supplment_0.PDF), тематических исследованиях по применению международного права в киберпространстве, опубликованных в феврале 2020 года (https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studieson-the-application-of-international-law-incyberspace.pdf), Стратегии международного взаимодействия Австралии в киберпространстве и по вопросам критически важных технологий 2021 года и материалах по международному праву, представленных Австралией в качестве приложения к докладу Группы правительственных экспертов 2021 года по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности (пока не опубликовано).

Взаимодействие с участием многих заинтересованных сторон

Австралия признает важную роль сообщества с участием многих заинтересованных сторон, включая гражданское общество, частный сектор, научные круги и техническое сообщество, в содействии процессу формирования свободного, открытого, безопасного, стабильного, доступного и мирного киберпространства.

В связи с этим Австралия присоединилась к числу соавторов инициативы «ЛетсТокСайбер» (letstalkcyber.org), предоставившей платформу для участия многих заинтересованных сторон в деятельности Рабочей группы открытого состава и для взаимодействия с ней, а также для консультаций между государствами, гражданским обществом, частным сектором, научными кругами и техническим сообществом. Австралия также провела несколько раундов национальных консультаций с участием многих заинтересованных сторон и активно интересовалась мнениями сообщества многих заинтересованных сторон для обоснования своей позиции в процессах, осуществлявшихся в рамках Рабочей группы открытого состава и Группы правительственных экспертов.

Кроме того, Австралия создала сеть «Квод тек нетворк», целью которой является поддержка исследований и поощрение взаимодействия между государствами и партнерами из научно-образовательных и аналитических центров Австралии, Индии, Соединенных Штатов Америки и Японии по вопросам использования киберпространства и критически важных технологий. Сеть «Квод тек нетворк» будет выполнять исследования и выносить рекомендации, актуальные для разработки политики; углублять и укреплять понимание обществом вопросов, касающихся киберпространства и критически важных технологий; а также способствовать налаживанию информированного общественного диалога. Началом работы Сети стала публикация 9 февраля серии общедоступных статей, затрагивающих вопросы международного мира и безопасности, взаимосвязанности и региональной устойчивости к потрясениям, прав человека и этики, а также национальной безопасности (www.internationalcybertech.gov.au/node/139).

Колумбия

[Подлинный текст на испанском языке]
[31 мая 2021 года]

В соответствии с резолюцией 75/32 Организации Объединенных Наций, касающейся поощрения ответственного поведения государств в киберпространстве в контексте международной безопасности, Колумбия, исходя из оценок и рекомендаций, содержащихся в докладах Группы правительственных экспертов, представляет Генеральному секретарю свои мнения и замечания по следующим вопросам:

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

содержание концепций, упомянутых в докладах Группы правительственных экспертов.

В этой связи следует уточнить, что настоящий доклад дополняет доклад, который был представлен в 2020 году, и особое внимание в нем уделяется событиям, произошедшим за последний год, в основном в связи с рекомендациями, сформулированными в докладе Группы правительственных экспертов за 2015 год для рассмотрения государствами в целях содействия созданию открытой, безопасной, стабильной, доступной и мирной среды в области информационно-коммуникационных технологий (ИКТ).

Добровольные нормы, правила и принципы ответственного поведения государств

В соответствии с целями Организации Объединенных Наций, включая поддержание международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по повышению уровня стабильности и безопасности при использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных поставить под угрозу международной мир и безопасность.

Кроме того, аспекты освоения были включены в Национальную политику обеспечения доверия и безопасности в цифровой среде (документ № 3995/2020 Национального совета по социально-экономической политике), в качестве одной из основных целей которой указано укрепление потенциала в плане обеспечения цифровой безопасности граждан в государственном и частном секторах.

В этой связи правительство Колумбии в лице Министерства информационных технологий и связи, Национальной службы профессиональной подготовки и Министерства национального образования провело ряд мероприятий на основе стратегии освоения в рамках следующих конкретных программ:

- в рамках программы Министерства информационных технологий и связи «Поговорим об электронном правительстве» (2020–2021 годы) были предприняты усилия по повышению осведомленности граждан о цифровой кибербезопасности путем организации 15 занятий, охвативших более 4000 человек. Кроме того, в 2020 году для предпринимателей и микро-, малых и средних предприятий были проведены три обучающих семинара по вопросам цифровой безопасности с участием 483 человек, в том числе 156 женщин. Также были проведены два семинара по конкретным аспектам модели информационной безопасности и конфиденциальности;

- в рамках «Месяца цифровой безопасности» было проведено несколько мероприятий, среди которых следует выделить четыре семинара по специальным вопросам урегулирования инцидентов, организованные при поддержке компании «Сиско» и Группы реагирования на чрезвычайные ситуации кибернетического характера в Колумбии; два семинара по вопросу о важности проведения ревизий и управления рисками в государственных организациях; два совещания в рамках программы «Поговорим об электронном правительстве», посвященные результатам мероприятия, которое было проведено совместно с Организацией американских государств (ОАГ); первое состоявшееся в Колумбии заседание Совета по инновациям в области кибербезопасности; и два ориентированных на широкую общественность обсуждения по темам «Рекомендации о том, как не стать жертвой киберпреступников» и «Правовой подход к дезинформации в Интернете». Наконец, совместно с ОАГ было проведено второе заседание Совета по инновациям в области кибербезопасности. В общей сложности в этих мероприятиях приняли участие 1040 человек, включая сотрудников государственных учреждений и конечных пользователей, причем 45 процентов участников составили женщины;

- в ходе мероприятия «Колумбия 4.0», которое состоялось в рамках Встречи главных специалистов по информации на высшем уровне 2020 года, собравшей технологических лидеров из государственных организаций, была проведена конференция «Как пережить COVID-19 и цифровую трансформацию, не став жертвой хакерской атаки», в которой приняли участие 490 человек. Также был проведен семинар «Передовая практика в области выявления угроз и реагирования на них на основе модели MITRE ATT&CK и XDR», в котором, по оценкам, около 40 процентов участников составляли женщины. В этом контексте были проведены мероприятия по повышению осведомленности о модели информационной безопасности и конфиденциальности, в которых приняли участие примерно 3196 должностных лиц из 1834 организаций, в том числе из 131 организации общенационального уровня и 1224 местных организаций;

- в рамках инициативы «Цифровые таланты», осуществляемой Министерством информационных технологий и связи, был проведен конкурс «Цифровые навыки — обучение кибербезопасности», целью которого являлся отбор колумбийских сотрудников для прохождения обучения и наращивания потенциала в области кибербезопасности. Для обучения специализированным навыкам были предложены два дипломных курса: i) курс по кибербезопасности для руководителей или управляющих; и ii) курс по кибербезопасности для технического персонала;

- Национальная служба профессиональной подготовки, со своей стороны, реализует следующие программы: «Безопасность компьютерных сетей»; «Управление базами данных и обеспечение их безопасности»; «Контроль за обеспечением цифровой безопасности»; «Разработка встроенного программного обеспечения на устройствах»; «Введение в системы обеспечения информационной безопасности в соответствии со стандартом ISO IEC 27001»; «Применение методов диагностики в области кибербезопасности»; и «Управление вопросами информационной безопасности»;

- Министерство образования провело мероприятия в области освоения технологий, связанные с распространением контента (использование социальных сетей, а также кампании и семинары с участием государственных организаций и микро-, малых и средних предприятий). Кроме того, были

налажены партнерские отношения с частным сектором и международное сотрудничество;

- помимо этого, была проведена работа по организации дипломных курсов, в которых приняли участие 2216 преподавателей, а стратегия обеспечения цифровой безопасности была включена в проект «Цифровое обучение» для учащихся начальной, основной и средней школы, в котором приняли участие 4093 учащихся, в том числе через портал «Колумбия учится», содержащий более 30 материалов.

Во исполнение рекомендации, согласно которой «государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с использованием ИКТ», правительство Колумбии провело следующие мероприятия:

- в рамках Национальной политики обеспечения доверия и безопасности в цифровой среде (документ № 3995/2020 Национального совета по социально-экономической политике) были учреждены — в качестве механизма координации и управления — «национальный координатор», функции которого выполняет Консультационное управление президента по экономическим вопросам и вопросам цифровой трансформации, и Комитет по цифровой безопасности — коллегиальный орган, в состав которого входят организации, занимающиеся вопросами цифровой безопасности, и цель которого заключается в изучении конкретных вопросов цифровой безопасности на стратегическом уровне в относящихся к его мандату следующих тематических областях: 1) политика и нормативно-правовая база в области цифровой безопасности; 2) защита и охрана объектов критически важной национальной киберинфраструктуры; 3) управление рисками в области цифровой безопасности; 4) отслеживание кризисов и киберугроз; 5) защита личных данных; 6) международные аспекты цифровой безопасности; и 7) стратегические связи для достижения цифровой безопасности;

- был создан единый командный пункт по вопросам цифровой безопасности, целью деятельности которого является обеспечение безопасности и сохранности технологической инфраструктуры и веб-сайтов государственного сектора во время проведения национальных праздников, выборов и других соответствующих мероприятий. Его целями являются: i) кибербезопасность граждан и защита государства от киберугроз; ii) профилактика, упреждение и судебное расследование; iii) предупреждение инцидентов в области кибербезопасности; iv) обеспечение стабильности правительственной и институциональной структуры; и v) совершенствование программного обеспечения. Были созданы протоколы реагирования на возможные сценарии атак, таких как распределенные атаки типа «отказ в обслуживании» (DDoS-атаки) на веб-порталы, веб-уязвимости и распространение фальшивых новостей;

- в координации с Сенатом Республики проводились мероприятия, в рамках которых было организовано обучение по формированию передовой практики в области использования виртуальных платформ.

Что касается наилучших путей сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществления других совместных мер по противодействию таким угрозам, то 16 марта 2020 года Колумбия присоединилась к Конвенции о киберпреступности, принятой в Будапеште в 2001 году и вступившей в силу для страны 1 июля 2020 года. В настоящее время ведется работа по ее осуществлению.

Что касается принятия надлежащих мер для защиты критически важной инфраструктуры от угроз в сфере ИКТ, то Колумбия приняла необходимые меры в целях защиты государственных учреждений путем укрепления сформированной правительством группы реагирования на инциденты в области кибербезопасности. Реализуемый в этой связи проект предусматривает структурирование процесса, в рамках которого предполагается найти комплексное решение, обеспечивающее повышение эффективности предоставления государственным учреждениям услуг правительственной группой реагирования на инциденты в области кибербезопасности, с тем чтобы добиться большей отдачи на всей территории страны посредством совершенствования инфраструктуры информационных технологий, физической инфраструктуры и кадрового потенциала при гарантированном круглосуточном функционировании.

Предлагаемые инициативы включают проведение диагностики текущего состояния и разработку плана непрерывного совершенствования собственного оперативного, административного, кадрового и научного потенциала и технологической инфраструктуры в целях привлечения ресурсов для повышения компетентности этих учреждений в вопросах цифровой безопасности. Также разработан проект передислокации и оптимизации деятельности сформированной правительством группы реагирования на инциденты в области кибербезопасности.

Кроме того, с учетом рекомендации о том, что государства должны способствовать ответственному представлению информации о факторах уязвимости в сфере ИКТ и делиться соответствующей информацией о существующих методах борьбы с такими факторами уязвимости, чтобы ограничить, а по возможности и устранить, потенциальные угрозы для ИКТ и зависящей от ИКТ инфраструктуры, Колумбия способствует ответственному представлению информации о факторах уязвимости в сфере ИКТ и принимает разумные меры для обеспечения целостности цепочки поставок и предотвращения распространения скрытых вредоносных инструментов, методов или функций в сфере ИКТ в рамках работы с ОАГ и Организацией экономического сотрудничества и развития.

В новом документе с изложением государственной политики (документ № 3995/2020 Национального совета по социально-экономической политике) под названием «Национальная политика обеспечения доверия и безопасности в цифровой среде» предусмотрены конкретные действия по созданию модели регулярного раскрытия информации о факторах уязвимости во всех секторах, охватывающей контактные центры, связывающие собственников и операторов активов, поддерживающих критически важную деятельность, с соответствующими государственными правительственными структурами. В разработке этой модели будут принимать участие многие заинтересованные стороны, а также будет учтен международный опыт в этой области.

Что касается рекомендации о том, что государства не должны осуществлять или заведомо поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп реагирования на чрезвычайные ситуации (также именуемым группами реагирования на чрезвычайные ситуации кибернетического характера или группами реагирования на инциденты в сфере информационной безопасности) другого государства, а также о том, что государство не должно использовать уполномоченные группы реагирования на чрезвычайные ситуации для осуществления злонамеренной международной деятельности, то Колумбия, считая своей главной обязанностью обеспечение безопасной и мирной среды в сфере информационно-коммуникационных технологий, приняла меры, соответствующие международному праву и предусмотренные в Уставе Организации Объединенных Наций.

Так, в марте 2021 года правительство Колумбии издало Постановление № 500 и Президентскую директиву № 3, установив руководящие принципы и стандарты для стратегии обеспечения цифровой безопасности и утвердив модель безопасности и конфиденциальности в качестве инструмента осуществления политики в отношении электронного правительства.

В статье 16 Декрета № 2106 от 2019 года содержатся правила по упрощению, устранению и реформированию не являющихся необходимыми операций, процессов и процедур, существующих в органах государственного управления, и говорится, что для применения электронного документооборота и сохранения информации органы власти, в соответствии с руководящими принципами, изданными Министерством информационных технологий и связи, должны разработать стратегию обеспечения цифровой безопасности.

В рамках модели информационной безопасности и конфиденциальности, являющейся инструментом осуществления политики в отношении электронного правительства, Министерство информационных технологий и связи предоставляет общие рекомендации по ее внедрению, руководство по управлению рисками в области информационной безопасности и процедуру урегулирования инцидентов в сфере цифровой безопасности, устанавливая тем самым руководящие принципы и стандарты для стратегии обеспечения цифровой безопасности.

Перед лицом возможной кибератаки Колумбия осуществляет меры, подразумевающие применение правовых, разведывательных и дипломатических инструментов с целью остановить атаку и предотвратить разрушение имущества или гибель людей, используя все варианты защиты сети перед проведением той или иной операции в киберпространстве.

При разработке национальной политики обеспечения цифровой безопасности правительство Колумбии сосредоточило свои усилия на трех основных компонентах: i) создании потенциала в плане управления рисками в цифровой среде; ii) развитии институциональной системы в поддержку структуры управления; и iii) оценке планов действий и передового международного опыта. Для достижения этой цели предлагается следовать стратегии, предусматривающей следующее:

- разработку диагностики текущего состояния и плана постоянного укрепления собственного оперативного, административного, кадрового и научного потенциала и совершенствования технологической инфраструктуры;
- формулирование руководящих принципов создания цифровой сети для участия гражданского общества, предоставляющей различным заинтересованным сторонам возможность взаимодействовать и сотрудничать в борьбе с киберугрозами, укрепляя и наращивая потенциал Колумбии в плане обеспечения цифровой безопасности в рамках международного права;
- координирование разработки руководящих принципов в отношении планов повышения уровня цифровой безопасности в целях укрепления потенциала комплексной системы социального обеспечения в области обработки информации, а также управления и обмена ею с учетом состояния критически важной киберинфраструктуры комплексной системы социального обеспечения;
- формулирование в рамках национальной модели урегулирования инцидентов руководящих принципов, содержащих особые условия управления рисками и инцидентами в области цифровой безопасности, связанными с обработкой информации, а также с управлением и обменом ею в рамках комплексной системы социального обеспечения, причем эти условия должны

быть интегрированы в общую процедуру урегулирования инцидентов, установленную Комитетом по цифровой безопасности;

- координирование процесса интеграции соответствующих механизмов (технических, правовых, организационных и т. д.), позволяющих собирать необходимые цифровые свидетельства в случае любого инцидента кибернетического характера, затрагивающего обработку информации и управление и обмен ею в рамках подсистемы здравоохранения комплексной системы социального обеспечения;

- разработку, структурирование и представление проекта учреждения группы реагирования на инциденты в области кибербезопасности в секторе комплексного социального обеспечения;

- разработку, структурирование и представление проекта учреждения группы реагирования на инциденты в области кибербезопасности в системе разведывательных органов с целью обеспечить ее участие в охране национальной безопасности в цифровой сфере;

- разработку предложения по созданию на национальном уровне единого центрального журнала регистрации инцидентов в области цифровой безопасности, обеспечивающего возможность проведения анализа типологии инцидентов и периодической оценки необходимости выявления приоритетных стратегий и ресурсов для управления ими. В этом едином центральном журнале регистрации инцидентов должны быть сведены воедино имеющиеся отчеты об инцидентах в этой области, составленные различными заинтересованными сторонами, и при этом предполагается упростить подачу информации, которой обмениваются стороны, а также выявить надежные средства ее доставки и обеспечения конфиденциальности, сохранности и надлежащего использования.

Прилагаются усилия к тому, чтобы гарантировать соблюдение конституционных прав и свобод граждан в контексте получения и использования информации в соответствии с Политической конституцией страны.

В законодательстве Колумбии были приняты меры по установлению уголовной ответственности за следующие деяния: i) умышленный и несанкционированный доступ ко всей компьютерной системе или к ее части; ii) умышленное и несанкционированное повреждение, удаление, порча, изменение или изъятие компьютерных данных; iii) умышленный и несанкционированный перехват компьютерных данных, совершенный с помощью технических средств; и iv) производство и распространение или передача детской порнографии.

Был достигнут прогресс в разработке четкого определения национальной и международной критически важной инфраструктуры с выделением секторов, продукты или услуги которых признаются объектами критически важной инфраструктуры, а также в ведении перечня критически важных активов. В качестве меры по укреплению доверия эти определения представляются вниманию международного сообщества.

Параллельно ведется работа по созданию сетей урегулирования кризисов в соответствующих государственных органах, запрашивающих поддержку по этому вопросу. С этой целью также планируется наладить взаимодействие с международным сообществом посредством создания сети контактных центров «на политическом и техническом уровнях». В этой связи Колумбия:

- спланировала национальные и международные учения по обеспечению кибербезопасности, с тем чтобы, проводя такие совместные учения в этой области, регулярно проверять свою способность поддерживать связь с

другими государствами, а также способность отвечать на запросы о предоставлении помощи и смягчении последствий (в частности, применяя каналы связи, протоколы и процедуры);

- приняла участие в проведении учений «СайберЭКС» и «СайберДрилз» Международного союза электросвязи и координирует с Объединенным кибернетическим командованием проведение национальных учений по действиям в кризисных ситуациях;
- использовала заранее созданные национальные многосторонние сети по урегулированию кризисов и применяла опыт смягчения последствий, накопленный государством и негосударственными субъектами в ходе проведения кибероперации такого типа, опираясь на существующую передовую практику в области информирования об инцидентах в национальном и международном контексте;
- организовала совместные учения с различными ассоциациями. После атак, произошедших в разгар социальных протестов в киберпространстве и принявших форму угроз со стороны групп «хактивистов» как в адрес правительства, так и в отношении частных предприятий, Колумбийская федерация индустрии программного обеспечения и информационных технологий обратилась к правительству от имени группы компаний с предложением разработать специальные решения в области цифровой безопасности. После этих обращений был проведен ряд встреч, на которых рассматривались конкретные направления деятельности по оказанию возможной поддержки правительству, для чего среди аффилированных компаний был проведен опрос относительно возможностей разведки и мониторинга.

В контексте налаживания международного взаимодействия в случае злонамеренной кибероперации против критически важной инфраструктуры правительство Колумбии провело совместную работу с Соединенными Штатами.

Добровольные меры по укреплению доверия

Что касается расширения сотрудничества, в том числе создания координационных центров для обмена информацией о случаях злонамеренного использования ИКТ и оказания помощи в проведении расследований, то, действуя через Полицейский кибернетический центр при Управлении по расследованию уголовных преступлений и Международную организацию уголовной полиции (Интерпол), Национальная полиция, исходя из трех важнейших составляющих кибербезопасности (профилактика, проведение расследований и выполнение компьютерно-технической экспертизы), координирует свою деятельность с различными структурами, входящими в Комитет по цифровой безопасности при правительстве страны.

Это позволило добиться в 2020 и 2021 годах следующих результатов: провести 32 оперативные кампании по борьбе с киберпреступностью, произведя 219 арестов за преступления, связанные с использованием компьютеров; привлечь внимание к 14 072 инцидентам в сфере кибербезопасности через круглосуточную службу информирования полиции «КАИ виртуал»; выполнить запросы о блокировке 7139 веб-сайтов, содержащих материалы со сценами сексуального надругательства над детьми, и 1648 страниц, посвященных незаконным азартным играм; и выпустить 454 информационных бюллетеня.

Следует отметить, что сотрудничество активизировалось после создания ряда объединенных командных пунктов по вопросам цифровой безопасности, действующих под руководством Центра развития потенциала Колумбии в

области кибербезопасности, в целях концентрации различных возможностей в сфере кибербезопасности и кибероборонs на территории страны.

В упомянутом выше полицейском подразделении была разработана Комплексная стратегия обеспечения кибербезопасности, направленная на активную координацию действий между центральными органами судебной полиции и 51 децентрализованным подразделением уголовного розыска в целях стандартизации методов расследования, а также инструментов и механизмов активного сотрудничества.

По информации, полученной от Генеральной прокуратуры, с 2009 года наблюдается тенденция к росту числа преступлений, связанных с использованием компьютеров, причем в 2019 году их рост усилился. Так, если в 2018 году было зарегистрировано 22 238 преступлений, связанных с использованием компьютеров, то в 2019 году — 24 197, то есть на 9 процентов больше. В 2020 году эта тенденция закрепилась. В период с 1 января по 31 декабря было совершено 35 346 преступлений, связанных с использованием компьютеров, что свидетельствует об увеличении их числа на 70 процентов. Из вышесказанного можно сделать вывод о том, что во время пандемии в стране участились случаи совершения преступлений, связанных с использованием компьютеров.

Таким образом, для обмена информацией между Генеральной прокуратурой и Полицейским кибернетическим центром налажен постоянный канал связи, который можно рассматривать как круглосуточный контактный центр, созданный в соответствии со статьей 35 Конвенции о киберпреступности.

В целях повышения эффективности взаимодействия этих двух структур Центр развития потенциала Колумбии в области кибербезопасности при полиции провел обучение подразделений Генеральной прокуратуры, отвечающих за борьбу с киберпреступлениями, ознакомив сотрудников этих подразделений с возможностями, которыми располагает Полицейский кибернетический центр.

Кроме того, как уже упоминалось выше, государственная политика (документ № 3995/2020 Национального совета по социально-экономической политике) направлена на совершенствование стратегии в области кибербезопасности и кибероборонs и международного сотрудничества. Также ожидается, что применение таких механизмов реагирования на кризисные ситуации, как объединенные командные пункты, позволит усовершенствовать процесс обмена информацией, укрепить сотрудничество и обеспечить надежную, эффективную и своевременную координацию деятельности заинтересованных сторон в области кибербезопасности на национальном уровне.

Что касается сотрудничества, то прокуратура намерена расследовать преступления, связанные с использованием компьютеров, в первоочередном порядке, реагируя в соответствии с национальным и международным правом на запросы других государств об оказании помощи в расследовании преступлений, совершенных в сфере ИКТ или с использованием этих технологий в террористических целях, а также в смягчении последствий злонамеренной деятельности в области ИКТ на ее территории, о чем говорится в стратегическом руководстве Генеральной прокуратуры страны на 2020–2024 годы — разработанном Генеральным прокурором плане, в котором он комплексно описывает предусмотренные направления деятельности этого органа на ближайшие годы. С этой целью будет разработана стратегия, направленная на повышение квалификации дознавателей и сотрудников прокуратуры, занимающихся расследованием подобных дел, и на координацию их деятельности.

Так, информацию о киберпреступлениях, основанную на статистических данных, собираемых ежемесячно с момента вступления в силу Закона № 1273 от 2009 года и до настоящего времени, можно найти в разделе «Открытые данные Генеральной прокуратуры: поиск и скачивание» в разбивке по таким параметрам, как вид преступления по Уголовному кодексу Колумбии, год поступления сообщения о преступлении в прокуратуру или год совершения преступления, департамент, в котором произошли указанные события, статус и процессуальная стадия дела, а также пол и возрастная группа жертв или обвиняемых. Также предусмотрены идентификаторы, позволяющие установить, в каких криминальных вестниках содержатся формулировки предъявленных обвинений и обвинительных приговоров, а также представлены ордера на арест и файлы, свидетельствующие о нетипичности дела или об отсутствии состава преступления.

Подразделения Генеральной прокуратуры, которые занимаются расследованием преступлений, связанных с использованием компьютеров, на национальном уровне в основных городах страны, отвечают за обработку, анализ и сохранение цифровых улик, а также за проведение различных расследований связанных с использованием компьютеров преступлений, которые, в силу места их совершения, относятся к их подведомственности, и, среди прочего, за расследование таких дел, как похищение имущества с использованием компьютеров и распространение детской порнографии. В ходе этих расследований данные подразделения должны проводить допросы, осмотры, обыски, проверки, выезды на место происшествия, изъятия и задержания, а также осуществлять сопровождение задержанных на судебные заседания. Они также должны оказывать поддержку всем подведомственным подразделениям в работе по извлечению цифровых улик с устройств или веб-сайтов, а также по сохранению этих улик во всех необходимых случаях, включая расследование таких преступлений, как убийство, половые акты с несовершеннолетними в возрасте до 14 лет, порнография с участием несовершеннолетних в возрасте до 18 лет, а также, в особых случаях, при расследовании дел о клевете и оскорблениях.

Управление по международным делам Генеральной прокуратуры рассматривает все заявки об оказании юридической помощи, опираясь в большинстве случаев на положения Конвенции о киберпреступности и применяя на предварительных этапах критерии и параметры, содержащиеся в *Практическом руководстве по истребованию электронных доказательств через границы, совместно разработанном Управлением Организации Объединенных Наций по наркотикам и преступности*, Исполнительным директоратом Контртеррористического комитета и Международной ассоциацией прокуроров и переведенном на испанский язык при поддержке ОАГ.

Кроме того, через Центр развития потенциала Колумбии в области кибербезопасности, являющийся круглосуточным контактным центром по применению Конвенции о киберпреступности, удалось сделать Национальную полицию одним из основных субъектов международного сотрудничества, предоставив ей возможность поддерживать постоянные контакты по вопросам кибербезопасности с такими важными организациями, как Агентство Европейского союза по сотрудничеству правоохранительных органов и Интерпол, а также оказать поддержку различным учреждениям, стремящимся наладить практическое применение этого механизма сотрудничества.

Следует отметить, что через круглосуточный контактный центр планируется ускорить обработку запросов о взаимной правовой помощи, для чего в процесс вовлекаются 65 стран-членов и 13 стран-наблюдателей, входящих в данное соглашение о сотрудничестве.

Ниже будет сделана ссылка на рекомендацию о том, что при существующих темпах развития ИКТ и масштабах угрозы возникает необходимость в улучшении общего понимания и активизации сотрудничества. В этой связи рекомендуется регулярно проводить под эгидой Организации Объединенных Наций институциональный диалог с широким участием, а также диалоги на двусторонних, региональных и многосторонних форумах и в рамках других международных организаций.

В этой связи Колумбия продолжает активно участвовать в многосторонних диалогах в рамках Организации Объединенных Наций и других международных форумов, в первую очередь по вопросам, связанным с ответственным поведением государств в киберпространстве и с развитием информационно-коммуникационных технологий в контексте международной безопасности.

Сегодня, в условиях беспрецедентной глобальной взаимосвязанности, государства находятся в отношениях всеобщей взаимозависимости, совместно решая ряд проблем, противостоять которым в одиночку было бы им не по силам. С учетом этого государствам необходимо сделать выбор в пользу международного сотрудничества в области кибербезопасности, поскольку очевидно, что распространение и использование информационных технологий и средств распространения информации затрагивает интересы всего международного сообщества. По этой причине государствам следует действовать в общих интересах, поощряя использование информационно-коммуникационных технологий в мирных целях и предотвращая конфликты, возникающие в результате применения этих технологий. Для этого необходимо:

- оказывать содействие в создании потенциала в сфере информационно-коммуникационных технологий, что требуется для обеспечения международной безопасности, путем расширения возможностей государств в организации сотрудничества и коллективных действий, поощряя мирное использование этих технологий на основе международного сотрудничества под руководством группы реагирования на инциденты в области кибербезопасности;

- создать механизмы, обеспечивающие участие частного сектора, научных кругов и организаций гражданского общества, с тем чтобы они могли вносить вклад в усилия в информационно-коммуникационной сфере в контексте международной безопасности, при участии всех государств.

Что касается осуществления добровольного сотрудничества в двусторонних, многосторонних или региональных организациях, то для повышения эффективности добровольного сотрудничества и укрепления доверия, с тем чтобы государства могли совместно противостоять угрозам, связанным с использованием информационно-коммуникационных технологий, на национальном и международном уровнях, то правительство Колумбии в лице Министерства информационных технологий и связи проделало следующую работу:

- принимало участие в региональных программах, таких как круглый стол по кибербезопасности Сети электронного правительства стран Латинской Америки и Карибского бассейна, и поддерживало сотрудничество с ОАГ;

- с 2017 года принимало участие в реализации проекта «Профессиональная карьера в области кибербезопасности» (координатором проекта выступает Программа кибербезопасности ОАГ, а за его финансирование отвечает Фонд «Сити»; проект охватывает пять стран: Бразилию, Доминиканскую Республику, Колумбию, Коста-Рику и Перу), нацеленного на обучение малообеспеченных молодых людей в возрасте от 18 до 25 лет и на оказание содействия в их профессиональной подготовке в этой области;

- разработало инициативу «Девушки-хакеры», направленную на поддержку и создание возможностей для образования и трудоустройства женщин на основе расширения их знаний в областях, связанных с кибербезопасностью. В рамках этой инициативы Министерство информационных технологий и связи формирует отвечающую установленным требованиям группу женщин — высококлассных экспертов в области цифровой безопасности в Колумбии, которые в будущем войдут в состав «Колумбийской команды девушек-хакеров», что, с учетом участия в программе более 350 женщин — экспертов в области безопасности, позволит позиционировать страну как регионального лидера в реализации инициатив такого рода;

- создало площадку для диалога в рамках Совета по инновациям в области кибербезопасности, на которой региональные эксперты и специалисты по «дизайн-мышлению» (design thinking) провели два мероприятия с участием старших руководителей из государственного и частного секторов, профессиональных объединений и научных кругов в целях содействия развитию инноваций, повышения осведомленности участников и распространения передового опыта в области обеспечения кибербезопасности в регионе. Эти советы по инновациям созданы в рамках соглашения Программы кибербезопасности ОАГ с компанией «Сиско» и проводятся при поддержке ОАГ.

В контексте приверженности коллективным действиям с целью превратить Интернет в более безопасное место посредством содействия оказанию технической помощи со стороны технологических компаний для защиты гражданского населения, поскольку основная часть нападений приходится именно на частную собственность гражданских лиц, правительство Колумбии в лице Министерства информационных технологий и связи осуществляет программу «Верю в ИКТ», направленную на развитие цифровых навыков для уверенного противостояния рискам, связанным с использованием Интернета и ИКТ, и стимулирование использования и освоения Интернета в целях формирования позитивного цифрового следа. Эта программа предназначена для женщин и мужчин в возрасте от 6 до 28 лет и предусматривает дифференцированные стратегии в рамках виртуальных и очных рабочих сессий, позволяя бенефициарам развивать навыки выявления рисков и способствуя сосуществованию и активной деятельности в цифровой среде, а также использованию технологических инструментов для формирования солидарности и достижения благих целей в Интернете.

Кроме того, правительство Колумбии в лице Министерства информационных технологий и связи обеспечивает специализированную подготовку в области информационной безопасности для государственных организаций, которые обращаются за поддержкой к группе реагирования на инциденты в области кибербезопасности, и расширяет направления исследований в области кибербезопасности, укрепляя оперативный, административный, кадровый и научный потенциал и совершенствуя физическую и технологическую инфраструктуру, для чего:

– было принято руководство по консультативному сопровождению и иной поддержке процесса внедрения межсекторального механизма обеспечения информационной безопасности и конфиденциальности для организаций, основанного на политике в отношении электронного правительства, с инструментами, базирующимися на: i) модели информационной безопасности и конфиденциальности; и ii) модели рисков в области цифровой безопасности, — Руководстве по противодействию рискам и разработке механизмов контроля в государственных учреждениях Административного департамента государственного управления;

– была разработана стратегия внедрения политики обеспечения цифровой безопасности, сформулированная по результатам проведения семинаров и информационно-просветительских дискуссий, создания интерактивных инструментов и организации учебных курсов;

– правительственная группа реагирования на инциденты в области кибербезопасности предоставляет услуги по упреждающему, реактивному и базовому управлению вопросами безопасности всем государственным структурам, генерируя предупреждения и оповещения об угрозах и факторах уязвимости, обрабатывая и анализируя инциденты и принимая меры реагирования и координируя действия в связи с ними, а также укрепляя знания в области безопасности и формируя культуру цифровой безопасности среди всех гражданских служащих и уполномоченных по вопросам цифровой безопасности;

– опираясь на собственный портфель услуг, правительственная группа реагирования на инциденты в области кибербезопасности предоставляет сопровождение и поддержку государственным учреждениям в целях совершенствования процессов обеспечения безопасности технологической инфраструктуры, урегулирования инцидентов в области кибербезопасности и обеспечения осведомленности в вопросах цифровой безопасности. Правительственная группа реагирования на инциденты в области кибербезопасности состоит из группы технических специалистов, которые осуществляют и разрабатывают действия, направленные на предотвращение и урегулирование инцидентов в области кибербезопасности.

Международное сотрудничество и помощь в области обеспечения безопасности и наращивания потенциала в сфере информационно-коммуникационных технологий

Что касается содействия трансграничному сотрудничеству в целях устранения факторов уязвимости в критически важной инфраструктуре за пределами национальных границ, то Генеральная прокуратура страны отметила, что в настоящее время большое значение для борьбы с киберпреступностью имеет наращивание регионального потенциала. По этой причине Колумбия предприняла усилия по созданию стратегических партнерств и участию в различных инициативах, включая официальное присоединение к числу государств — участников Конвенции о киберпреступности, участие в деятельности различных рабочих групп Организации Объединенных Наций и подписание с различными государствами меморандумов о взаимопонимании в деле борьбы с киберпреступностью.

Кроме того, в рамках сотрудничества и координационных усилий Колумбия взаимодействует с группой реагирования на инциденты в области кибербезопасности в Западном полушарии, служащей площадкой для обмена информацией об угрозах и совместной работы существующих в регионе групп реагирования на инциденты.

Колумбия также участвует в международных проектах по обмену информацией, в том числе в проектах, связанных с выпуском бюллетеней и созданием систем раннего предупреждения правительственных и надзорных органов финансового сектора в других странах региона (Центральноамериканского совета контролеров банков, страховых компаний и других финансовых учреждений и Тихоокеанского альянса).

Генеральная прокуратура способствовала подписанию с другими государствами ряда меморандумов о взаимопонимании в области борьбы с киберпреступностью и иными сопутствующими преступлениями.

Что касается содействия продолжению деятельности по наращиванию потенциала, в частности в сфере проведения криминалистической экспертизы или принятия совместных мер по противодействию преступному или террористическому использованию ИКТ, то работа по совершенствованию технологий и наращиванию потенциала велась не так оперативно по причине высокой стоимости лицензирования, закупаемого оборудования и необходимого обучения.

В ответ на рекомендацию о том, что в интересах наращивания потенциала в плане обеспечения безопасности в сфере ИКТ государства могли бы рассмотреть вопрос о выдвижении инициатив по двустороннему и многостороннему сотрудничеству, которое бы основывалось на существующих партнерских отношениях, и о том, что такие инициативы могли бы способствовать улучшению условий для оказания эффективной взаимопомощи между государствами в их деятельности по реагированию на инциденты в сфере ИКТ и могли бы далее развиваться компетентными международными организациями, включая Организацию Объединенных Наций и ее учреждения, частный сектор, научные круги и организации гражданского общества, правительство Колумбии в лице Министерства информационных технологий и связи возглавило Исполнительный комитет Сети электронного правительства стран Латинской Америки и Карибского бассейна, обеспечивающий взаимодействие органов электронного правительства 34 стран региона в области кибербезопасности.

Чтобы оценить положение дел в сфере кибербезопасности и предложить к утверждению действия, направленные на повышение уровня кибербезопасности в странах — членах Сети и в регионе, предлагается принять следующие меры:

– проверить степень надежности систем обеспечения кибербезопасности (исследование Межамериканского банка развития и ОАГ);

– проверить уровень подготовки групп реагирования на связанные с компьютерами чрезвычайные ситуации и групп реагирования на инциденты в области кибербезопасности (SIM3);

– создать архивное хранилище для руководств, процедур и примеров передового опыта в области кибербезопасности;

– провести мероприятие по кибербезопасности для лиц, ответственных за принятие решений;

– сформулировать региональные стратегии обеспечения кибербезопасности;

– выявлять добровольно применяемые в регионе передовые методы работы с конфиденциальными данными (поощрение использования трансграничной электронно-цифровой подписи и повышение операционной совместимости);

– проанализировать состояние групп реагирования на инциденты в области кибербезопасности членов Сети;

– сформировать отраслевые группы реагирования на инциденты в области кибербезопасности и наладить региональное сотрудничество;

– укрепить потенциал в области кибербезопасности;

– укрепить потенциал групп реагирования на инциденты в области кибербезопасности;

– создать площадку для обмена информацией о вредоносном программном обеспечении (группа реагирования на инциденты в области кибербезопасности в Западном полушарии);

– провести анализ региональных механизмов защиты данных.

Кроме того, правительство Колумбии по согласованию с ОАГ и Министерством информационных технологий и связи реализовало ряд предложений по модели управления в области цифровой безопасности и одобрило методическое руководство по выявлению рисков в области цифровой безопасности и управлению ими при внедрении новейших технологий в Колумбии. В рамках этого предложения был достигнут прогресс по следующим направлениям работы:

– составление перечней источников данных и справочных материалов для обоих предлагаемых продуктов;

– анализ передовой практики для подготовки обоих продуктов посредством обучения перенятию опыта (benchlearning) в отношении моделей управления, применимых к сфере цифровой безопасности;

– анализ местных условий (институциональная система, заинтересованные стороны и т. д.);

– формулирование принципов и целей предлагаемой модели управления;

– подтверждение этих целей и получение предложений от различных заинтересованных сторон в отношении модели управления;

– выявление ожиданий различных заинтересованных сторон в отношении модели управления.

Следует отметить, что для оценки предложенных принципов и целей, а также интересов различных заинтересованных сторон в отношении модели управления в Колумбии в рамках официального заседания Комитета по цифровой безопасности, состоявшегося 30 октября 2020 года, было проведено первое рабочее совещание, в котором приняли участие представители более 80 представителей различных заинтересованных сторон, имеющих отношение к национальной экосистеме кибербезопасности.

Получив возможность создать платформу, обеспечивающую оперативное сотрудничество не только между государствами, но и с частным сектором страны, с целью противостоять крупномасштабным инцидентам и кризисам в области кибербезопасности и реагировать на них, правительство Колумбии во главе с Министерством национальной обороны ведет работу по уточнению положений плана действий, содержащегося в документе № 3995/2020 Национального совета по социально-экономической политике, что подразумевает:

a) разработку мер по укреплению доверия в цифровой сфере посредством повышения уровня цифровой безопасности, что позволит Колумбии сформировать инклюзивное и конкурентоспособное общество в цифровом будущем путем укрепления потенциала и модернизации системы управления цифровой безопасностью;

b) утверждение моделей, ориентированных на использование новых технологий и предусматривающих продолжение работы по технологическому внедрению Национальной системы урегулирования инцидентов в области кибербезопасности, в целях координации институциональных усилий по оперативному урегулированию инцидентов в области кибербезопасности и создания официального источника статистических данных о зарегистрированных в стране инцидентах такого рода;

c) стандартизацию работы механизма периодического информирования об инцидентах и факторах уязвимости в области кибербезопасности, что позволит их выявлять, оценивать и доводить до сведения заинтересованных сторон, а также обеспечит поступление информации для принятия решений национальным правительством.

Применение норм международного права в контексте использования информационно-коммуникационных технологий

Колумбия считает, что нормы международного права, в частности Устав Организации Объединенных Наций, а также нормы международного права прав человека и международного гуманитарного права, сообразно обстоятельствам, могут применяться к «виртуальному пространству» в той же мере, в какой они применяются к «физическому пространству». При этом международное гуманитарное право применяется только в условиях вооруженного конфликта (в физическом или виртуальном пространстве).

Нормы международного права, и в частности Устав Организации Объединенных Наций, применимы и имеют принципиальное значение в контексте поддержания мира и стабильности и создания открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. В связи с этим принцип суверенного равенства берется за основу для обеспечения максимальной безопасности при использовании ИКТ государствами, и необходимо соблюдать, среди прочих принципов международного права, принципы государственного суверенитета, суверенного равенства, мирного разрешения споров и невмешательства во внутренние дела других государств.

Концепции

Что касается уточнения концепций, связанных с международным миром и безопасностью в контексте использования ИКТ в правовой, технической и политической сферах, то с учетом особенностей применения и новизны этих концепций представляется необходимым продолжить их обсуждение в рамках многосторонних форумов, следуя выводам заключительного доклада Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, принятого консенсусом в марте 2021 года.

Чтобы глубже изучить вопрос о применении международного права в киберпространстве, необходимо располагать средствами наращивания потенциала, обеспечивающими всем государствам возможность говорить на одном языке и совершенствоваться в понимании того, как следует адаптировать международные нормы к задачам в отношении киберпространства и как сформировать консенсус по поводу применения норм международного права в этом виртуальном пространстве.

Особо важным представляется достижение прогресса в выполнении рекомендаций как групп правительственных экспертов, так и Рабочей группы открытого состава.

Кроме того, крайне важно обеспечить создание глобального механизма для регулярного институционального диалога в рамках Организации Объединенных Наций в интересах достижения прогресса в этом направлении, а также продолжение и активизацию работы, ведущейся на региональном уровне.

В этой связи следует отметить, что Колумбия входит в число соавторов инициативы по разработке программы действий в области ответственного использования ИКТ в контексте международной безопасности и оказывает

поддержку в ее реализации в качестве постоянного, инклюзивного, одобренного консенсусом международного нормативного документа, ориентированного на практические действия и поощряющего ответственное поведение при использовании ИКТ в контексте международной безопасности.

Дания

[Подлинный текст на английском языке]
[28 мая 2021 года]

В Дании, как и во многих других странах мира, цифровые решения являются частью повседневной жизни и способствуют экономическому росту. Для Дании, которая является одной из наиболее цифровизированных стран мира, жизненно важно содействовать формированию глобального, открытого, свободного, стабильного, мирного и безопасного киберпространства, в котором в полной мере соблюдались бы права человека, основные свободы и принцип верховенства права.

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

Дания предприняла ряд шагов по укреплению своей информационной безопасности и развитию международного сотрудничества в киберпространстве.

Оборонное соглашение на период 2018–2023 годов предусматривает выделение 1,4 млрд датских крон на цели укрепления кибербезопасности и кибероборонны, что позволит повысить устойчивость Дании к угрозам, возникающим в киберпространстве. В Национальной стратегии Дании в области кибернетической и информационной безопасности на 2018–2021 годы изложены дальнейшие шаги по укреплению кибербезопасности и информационной безопасности, предусматривающие осуществление систематических и скоординированных усилий. Посредством реализации 25 инициатив и шести целевых стратегий в секторах, определяемых как критически значимые (энергетика, финансы, транспорт, здравоохранение, телекоммуникации и морское судоходство), Дания усилила технологическую устойчивость своей цифровой инфраструктуры, повысила уровень соответствующих знаний и навыков своих граждан, предпринимателей и представителей органов власти, а также укрепила координацию и сотрудничество в области кибербезопасности.

В рамках Национальной стратегии в области кибернетической и информационной безопасности на 2018–2021 годы в шести вышеупомянутых важнейших секторах были сформированы специализированные подразделения по кибернетической и информационной безопасности. Кроме того, в рамках Национальной стратегии был создан форум для обмена опытом в области кибер- и информационной безопасности между специализированными секторальными подразделениями и Центром кибербезопасности. В работе форума также принимают участие Агентство по цифровизации и Датская служба безопасности и разведки.

В целях создания пула квалифицированных кадров, способных выявлять и отражать кибератаки, направленные против Дании, в частности против объектов ее критически важной инфраструктуры, Центр кибербезопасности создал Академию киберзащиты — учебное подразделение, на базе которого проводятся курсы интенсивной подготовки. Кроме того, Центр кибербезопасности оказывает поддержку в осуществлении образовательной и исследовательской деятельности в области кибербезопасности и по другим направлениям.

В дополнение к этим усилиям Агентство по цифровизации провело несколько учебных курсов и информационных мероприятий и разработало ряд методических руководств по кибербезопасности и информационной безопасности, ориентированных на сотрудников руководящего звена и специалистов в области кибербезопасности, а также государственных служащих.

В рамках Национальной стратегии в области кибернетической и информационной безопасности на 2018–2021 годы Агентство по цифровизации запустило сайт sikkerdigital.dk, на котором граждане могут ознакомиться с рекомендациями и статьями и воспользоваться обучающими программами по вопросам кибер- и информационной безопасности, а также получить актуальную информацию о различных угрозах. Помимо ведения этого веб-сайта Агентство по цифровизации в сотрудничестве с муниципальными и региональными органами проводит национальные кампании по обучению навыкам безопасного поведения в цифровом пространстве.

В Дании также действует Совет кибербезопасности — государственно-частное партнерство, созданное для консультирования правительства по вопросам укрепления кибербезопасности и улучшения обмена знаниями между органами власти и деловыми и научными кругами. В порядке осуществления Национальной стратегии в области кибернетической и информационной безопасности на 2018–2021 годы Дания расширила свое участие в международных усилиях в области кибербезопасности: так, в Брюссель были направлены атташе по кибербезопасности, в Министерстве иностранных дел был назначен координатор по международной кибербезопасности, в представительстве технического посла Дании в Кремниевой долине был назначен советник по кибербезопасности, а кроме того, Дания присоединилась к Центру передового опыта по совместной киберзащите Организации Североатлантического договора (НАТО) в Таллине. Это позволило Дании активизировать свое участие в межгосударственных форумах по вопросам кибербезопасности, которые проводят, например, Организация Объединенных Наций, Европейский союз, Организация Североатлантического договора и Организация по безопасности и сотрудничеству в Европе (ОБСЕ).

В настоящее время правительство Дании разрабатывает новую национальную стратегию в области кибернетической и информационной безопасности на период 2022–2024 годов. В рамках этой стратегии текущие усилия по укреплению кибербезопасности и информационной безопасности будут продолжены и расширены посредством реализации инициатив, ориентированных на работу с государственным и частным секторами и гражданами Дании.

Наряду с этим Дания в сотрудничестве со своими партнерами и союзниками по НАТО и Европейскому союзу продолжает участвовать в противодействии гибридным угрозам, таким как кибератаки и операции влияния. Ответом на рост числа таких атак и операций, отмеченный в период пандемии коронавирусного заболевания (COVID-19), стали постоянные дипломатические усилия по линии Организации Объединенных Наций, Европейского союза, НАТО и ОБСЕ, направленные на содействие планомерному построению свободного, открытого, стабильного, мирного и безопасного киберпространства. Кроме того, Дания является активным членом Группы сотрудничества в области сетевой информационной безопасности и сети групп реагирования на инциденты в области кибербезопасности, а также членом совета Европейского агентства по кибербезопасности.

Дания подчеркивает, что, как четко заявило международное сообщество, тема киберпространства прочно укоренилась в существующем международном праве, о чем свидетельствуют консенсусные доклады, подготовленные в 2013 и

2015 годах группами правительственных экспертов. Существующие рамки международного права, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека, применяются к поведению государств в киберпространстве и имеют важнейшее значение для поддержания мира и стабильности и формирования открытой, безопасной, мирной и доступной информационно-коммуникационной среды. Кроме того, Дания подчеркивает важность 11 добровольных и не имеющих обязательной силы норм ответственного поведения государств, сформулированных в докладе Группы правительственных экспертов от 2015 года, как дополняющих действующее международное право и проистекающих из него.

Несмотря на усилия, прилагаемые на национальном и международном уровнях, способность и готовность государственных и негосударственных субъектов осуществлять вредоносную деятельность в киберпространстве продолжает увеличиваться. Этой проблеме следует уделить самое широкое внимание. Вредоносная деятельность в киберпространстве может представлять собой международно-противоправное деяние и способна дестабилизировать обстановку и создать опасность эскалации. Дания по-прежнему преисполнена решимости предотвращать и пресекать злонамеренную активность в киберпространстве и реагировать на инциденты в области информационной безопасности и стремится к расширению международного сотрудничества в этой области. Дания поддерживает призыв Европейского союза, в котором он просил международное сообщество 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.

Содержание концепций, упомянутых в докладах Группы правительственных экспертов

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 вредоносной деятельности, осуществляемой государственными и негосударственными субъектами, а также увеличением числа случаев хищения интеллектуальной собственности, совершенных с использованием кибертехнологий. Такие действия угрожают экономическому росту и стабильности международного сообщества.

Никогда еще потребность в глобальном, свободном, открытом, безопасном, стабильном и мирном киберпространстве не была столь очевидна, как во время пандемии коронавирусного заболевания (COVID-19). Информационно-коммуникационные технологии позволяют осуществлять общение, сотрудничество и обмен знаниями, которые необходимы миру для борьбы с пандемией и преодоления ее последствий.

Тем не менее во время текущего кризиса, вызванного коронавирусным заболеванием (COVID-19), мы стали свидетелями того, что злоумышленники не гнушаются использовать для достижения своих целей любую возможность — даже глобальную пандемию. В частности, они подрывают работу критически важной инфраструктуры, включая больницы, играющие ключевую роль в борьбе с пандемией, и совершают хищения интеллектуальной собственности при помощи кибертехнологий. Любые попытки помешать функционированию

критически важных объектов 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, обеспечиваемых информационно-коммуникационными технологиями, так как это может повлечь за собой системные последствия. Такие злонамеренные действия неприемлемы и должны быть решительно осуждены всеми государствами. Кроме того, государства должны проявлять должную осмотрительность и принимать оперативные и решительные меры для пресечения вредоносной деятельности в сфере информационно-коммуникационных технологий, осуществляемой с их территории.

Кроме того, как признается в предыдущих докладах Группы правительственных экспертов и Рабочей группы открытого состава, ввиду уникального характера ИКТ подход Организации Объединенных Наций и государств-членов к борьбе с киберугрозами в контексте международной безопасности должен оставаться технологически нейтральным. Это соответствует признанной Организацией Объединенных Наций концепции, согласно которой существующее международное право применимо к новым областям, включая использование новых технологий.

Как международное право применяется в сфере использования информационно-коммуникационных технологий

Дания решительно поддерживает многостороннюю систему, в основе которой лежит опирающийся на правила международный порядок и которая предназначена для борьбы с существующими и потенциальными угрозами, возникающими в результате злонамеренного использования ИКТ.

Международное сообщество четко заявило о том, что тема киберпространства прочно укоренилась в существующем международном праве, о чем свидетельствуют консенсусные доклады групп правительственных экспертов от 2013 и 2015 годов. 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. Дания с удовлетворением отмечает, что в этом году Генеральная Ассамблея консенсусом подтвердила этот принцип, одобрив заключительный доклад Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Теперь все государства-члены должны выполнять взятое на себя обязательство.

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 для достижения консенсуса по данному вопросу и выработки единого подхода к нему предстоит сделать еще многое, и Дания поддерживает направленную на достижение этой цели деятельность, которая осуществляется по линии Группы правительственных экспертов, Рабочей группы открытого состава и других международных и региональных инициатив, таких как новая программа действий в целях поощрения 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 физическом

мире, так и в Интернете, 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 применимого международного права проведение киберпространственных операций не отличается от использования обычного военного потенциала. Это также отражено в национальном документе «Совместная доктрина военных киберпространственных операций» от 2019 года, в котором военным руководителям предписывается учитывать соображения соблюдения принципов международного права при проведении киберпространственных операций. Таким образом, международное гуманитарное право, включая принципы предосторожности, гуманности, военной необходимости, соразмерности и проведения различия, 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.

Существующее международное право, дополняемое 11 не имеющими обязательной силы добровольными нормами ответственного поведения, сформулированными в докладе Группы правительственных экспертов 2015 года, очерчивает рамки ответственного поведения государств в киберпространстве. Дания призывает все государства придерживаться этих рамок и выполнять включенные в них рекомендации.

Ввиду того, что существующая международно-правовая база применима к вопросам кибербезопасности, Дания не призывает разрабатывать новые международно-правовые инструменты в области кибербезопасности и не считает это необходимым. Вместе с тем выработка единой позиции в отношении порядка применения существующих норм международного права к деятельности в киберпространстве требует дальнейших усилий. Хочется надеяться, что работа и рекомендации действующей Группы правительственных экспертов и новой Рабочей группы открытого состава 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.

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 70/237, и продолжать применять согласованные нормы и принимать меры по укреплению доверия, которые играют важную роль в предотвращении конфликтов.

Огромное значение имеют нормы, правила и принципы ответственного поведения государств, которые были сформулированы в последовательных докладах Группы правительственных экспертов от 2010, 2013 и 2015 годов и которые дополняют международное право и проистекают из него. Дания будет и впредь руководствоваться международным правом, а также соблюдать эти добровольные нормы, правила и принципы. Дальнейшее осуществление этих норм должно обеспечиваться на основе расширения сотрудничества и повышения транспарентности в отношении передовой практики.

Республика Молдова

[Подлинный текст на английском языке]
[24 мая 2021 года]

Информационные технологии, информационные ресурсы и электронные коммуникационные системы стали неотъемлемой частью всех сфер деятельности человека, общества и государства. Информационные технологии способствуют коренным преобразованиям общественного устройства и служат катализатором для консолидации информационного общества на национальном, региональном и международном уровнях. Таким образом, информационные технологии вышли за юрисдикционные рамки, определяемые границами отдельных государств или государственных объединений.

Несмотря на неоспоримые преимущества современных технологий, информационное пространство подвержено ряду угроз в области безопасности. Так, оно является питательной средой для недобросовестной конкуренции, шпионажа, массовой дезинформации, пропаганды, терроризма и организованной преступности, а также для тиражирования различных проявлений ненависти и подстрекательства к насилию, особенно по признакам пола, расы, национальности, этнического происхождения, языка, религии, политической принадлежности и другим, чему, к сожалению, не придается должное значение и в отношении чего редко применяются меры противодействия или меры по исправлению положения.

Основными приоритетами национальной политики по обеспечению информационной безопасности в правовом государстве являются повышение уровня информационной безопасности и создание благоприятных условий для определенных направлений деятельности как государственных, так и частных субъектов, в том числе рядовых пользователей информационных систем. Выполнение этих приоритетных задач требует наличия актуальной и всеобъемлющей нормативно-правовой базы, которая охватывала бы все основные вопросы информационной безопасности. Руководствуясь этим пониманием, Республика Молдова утвердила Стратегию в области информационной безопасности и План деятельности по ее осуществлению. Целью Стратегии является обеспечение защиты основных прав и свобод, демократии и верховенства права в информационном пространстве.

Классификация рисков, угроз и факторов уязвимости, а также систематизация мер по обеспечению информационной безопасности способствуют повышению уровня доверия в киберпространстве, что нашло отражение в Стратегии в области информационной безопасности Республики Молдова.

Задача Стратегии — установить юридическую связь и обеспечить системную интеграцию между приоритетными направлениями и обязанностями и компетенциями в целях обеспечения информационной безопасности на национальном уровне на основе принципов киберустойчивости, плюрализма СМИ и институционального сближения в сфере безопасности с целью защиты суверенитета, независимости и территориальной целостности Республики Молдова.

Таким образом, Стратегия содержит конкретные и четкие механизмы выявления угроз информационной безопасности, противодействия им и реагирования на них, а также сроки выполнения поставленных в ней задач.

Механизмы и цели, предусмотренные Стратегией, ориентированы на создание и обновление нормативно-правовой базы и реализацию технической и программной составляющих, призванных противостоять вызовам внутри

страны и за ее пределами, а также на подготовку кадров и активизацию сотрудничества с национальными и международными компетентными органами.

В этой связи Стратегия предусматривает создание интегрированной системы оценки угроз в области информационной безопасности и оповещения о них, а также разработку мер оперативного реагирования. Это предполагает создание или назначение организации, которая возьмет на себя роль национального центра реагирования на инциденты в области кибербезопасности и будет служить для компетентных государственных органов и физических и юридических лиц единым пунктом для сигнализирования о киберинцидентах. Создание национальной группы по реагированию на чрезвычайные ситуации в киберпространстве позволит укрепить сеть групп реагирования на территории Республики Молдова и обеспечить быстрое реагирование на инциденты.

Кроме того, ввиду необходимости постоянного контроля и обеспечения высокого уровня кибербезопасности, Стратегия предусматривает проведение аудита объектов информационной инфраструктуры, имеющих национальную значимость, и внедрение международных стандартов в области информационной безопасности.

Помимо этого, Стратегия предусматривает механизмы защиты специальных коммуникационных сетей Республики Молдова и информации ограниченного доступа. Системы связи, информационные системы и сети передачи данных предназначены для хранения, обработки и дальнейшей передачи важных для государства данных, а потому требуют особого подхода в плане их защиты и развития.

Расширение арсенала средств криптографической защиты и усложнение криптографических алгоритмов обуславливают необходимость контроля за импортом, сертификацией и использованием средств защиты информации. В этой связи Стратегией предусмотрена обязательная сертификация технических и криптографических средств защиты информации, разработка систем контроля за импортом средств защиты информации, приведение национальных законов в области криптографической защиты информации в соответствие с европейской правовой базой и создания базы данных по техническим и криптографическим средствам защиты информации.

Кроме того, свободный доступ к глобальной сети Интернет, наличие в ней информации порнографического и экстремистского характера, а также сложность установления источника и проверки достоверности загруженных данных обуславливают необходимость разработки механизмов защиты пользователей, особенно детей, от любых форм злоупотреблений в онлайн-пространстве.

Для выявления угрозы информационной безопасности в медийном пространстве, противодействия этой угрозе и реагирования на нее был необходим анализ интернет-пространства на предмет выявления юридических и/или физических лиц, участвующих в создании и распространении контента, оказывающего влияние на информационную безопасность Республики Молдова

Что касается развития механизмов стратегической коммуникации, защиты национальных интересов Республики Молдова и обеспечения безопасности информационного медийного пространства, то Стратегия предусматривает проведение комплексного исследования, направленного на выявление и оценку факторов уязвимости медийного компонента системы информационной безопасности, а также создание стратегического информационно-коммуникативного ресурса для передачи информации об инцидентах в области безопасности и выявленных попытках дезинформации и/или манипулирования.

Кроме того, следует отметить, что важным компонентом Стратегии является укрепление международного сотрудничества в области информационной безопасности и противодействия киберпреступности.

В Стратегии в области информационной безопасности, утвержденной на период 2019–2024 годов, определен ряд целей и мер, подлежащих поэтапной реализации, в том числе при содействии международных партнеров.

При том что на национальном уровне Республика Молдова стремится внедрить ряд мер по укреплению своего потенциала в области информационной безопасности, на международном уровне, по нашим оценкам, ситуация в киберпространстве становится все более сложной: государственные субъекты, преследующие злонамеренные цели, проводят сложные кибератаки в целях вмешательства в избирательные процессы других стран, наносят ущерб критически важным объектам инфраструктуры и используют шпионские программы для атаки на производственно-сбытовые цепочки; все это является нарушением резолюций Организации Объединенных Наций.

Не отстают от них и негосударственные субъекты киберпространства, в полной мере эксплуатирующие уязвимости информационных систем в преступных целях для получения прибыли, используя модель «вредоносное ПО как услуга».

Вышеперечисленные проблемы заставляют население настороженно относиться к новым технологиям и препятствуют надлежащему развитию информационно-коммуникационной сферы.

Сингапур

[Подлинный текст на английском языке]
[24 мая 2021 года]

Сингапур твердо привержен идее установления в киберпространстве основанного на правилах международного порядка, который станет необходимым 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 безопасное, надежное, открытое и функционально совместимое киберпространство, действующее на основе применимых норм международного права, четко определенных стандартов ответственного поведения государств, эффективных мер укрепления доверия и скоординированных усилий по наращиванию потенциала. Важно продолжать обсуждение соответствующих законов, правил и норм в рамках Организации Объединенных Наций — единственного универсального, инклюзивного и многостороннего форума, где все государства имеют 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 недавно завершившей свою работу Рабочей группы открытого состава, учрежденной в соответствии с резолюцией 73/27 Генеральной Ассамблеи. Мы по-прежнему готовы вносить конструктивный вклад в деятельность Организации Объединенных Наций по разработке и внедрению норм и правил в области кибербезопасности и будем продолжать активно участвовать в соответствующих будущих процессах в рамках Организации. На наш взгляд, очень важно, чтобы при дальнейшем обсуждении вопросов кибербезопасности в Организации Объединенных Наций учитывался широкий спектр мнений, особенно мнений малых государств и

развивающихся стран, которые наиболее уязвимы к последствиям киберконфликтов. Для этого любой процесс, имеющий отношение к кибербезопасности, который будет проводиться в будущем на уровне Организации Объединенных Наций, должен быть открытым, инклюзивным и совместным, с тем чтобы еще больше укрепить международное сотрудничество и добиться 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 передовым опытом и содействия наращиванию потенциала Организации Объединенных Наций.

Сингапур считает, что государства должны содействовать повышению осведомленности о существующих добровольных необязательных нормах ответственного поведения государств и поощрять их соблюдение. Сингапур поддерживает дальнейшее совершенствование таких норм по мере необходимости. Например, критически важная трансграничная информационная инфраструктура, за защиту которых несут ответственность все государства-члены, может рассматриваться как особая категория критически важной инфраструктуры и должна быть охвачена в рамках существующего набора норм, поскольку ИКТ-угрозы для объектов такой инфраструктуры могут иметь дестабилизирующие последствия как на региональном, так и глобальном уровне[2].

Региональные организации могут играть важную роль в этом процессе. Ассоциация государств Юго-Восточной Азии (АСЕАН) подтвердила необходимость установления в киберпространстве международного порядка, основанного на правилах, в опубликованном в апреле 2018 года первом заявлении лидеров АСЕАН о сотрудничестве в области кибербезопасности. В сентябре 2018 года участники третьей Конференции на уровне министров стран — членов АСЕАН по вопросам кибербезопасности договорились принципиально поддержать 11 норм, содержащихся в докладе Группы правительственных экспертов от 2015 года, и сосредоточить внимание на укреплении регионального потенциала в области соблюдения этих норм. В октябре 2019 года участники четвертой Конференции на уровне министров стран — членов АСЕАН по вопросам кибербезопасности приняли решение создать рабочий комитет для рассмотрения вопроса о разработке долгосрочного регионального плана действий по обеспечению эффективной реализации этих норм на практике, в том числе в таких областях, как сотрудничество между группами реагирования на инциденты в области кибербезопасности, защита критически важной информационной инфраструктуры и взаимопомощь в вопросах кибербезопасности. Участники пятой Конференции на уровне министров стран — членов АСЕАН по вопросам кибербезопасности, состоявшейся в 2020 году, подтвердили обязательство АСЕАН разработать план действий по составлению «дорожной карты» реализации добровольных норм в подходящем для всех государств — членов АСЕАН темпе. Они также подтвердили настоятельную необходимость защищать объекты критически важной национальной и трансграничной информационной инфраструктуры.

Наращивание потенциала имеет ключевое значение для обеспечения того, чтобы отдельные государства могли успешно применять нормы ответственного поведения государств и выполнять свои обязательства по международному

[2] Критически важная трансграничная информационная инфраструктура — это критически важные объекты информационной инфраструктуры, принадлежащие частным компаниям и функционирующие на трансграничной основе, но не находящиеся под юрисдикцией какого-либо одного государства.

праву. В рамках этих усилий Сингапур в 2016 году 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. На сегодняшний день в рамках Программы прошли обучение более 600 должностных лиц из государств — членов АСЕАН. В 2019 году Программа была расширена за счет открытия Центра передового опыта АСЕАН-Сингапур в области кибербезопасности с финансированием в объеме 30 млн долл. США, который предлагает учебные программы стратегического и технического уклона для старших должностных лиц стран АСЕАН. Центр передового опыта начал функционировать с апреля 2020 года. Несмотря на ограничения на поездки, введенные в связи с пандемией COVID-19, Центр продолжил осуществлять учебную деятельность полностью в онлайновом режиме и в 2020 году организовал семь виртуальных курсов по наращиванию потенциала.

Кроме того, в рамках совместной программы Организации Объединенных Наций и Сингапура по кибернетической проблематике Сингапур выступил соорганизатором практикума, целью которого было повышение осведомленности о проблемах использования киберпространства среди государств — членов АСЕАН. Помимо этого, в партнерстве с Управлением по вопросам разоружения Сингапур разработал передовой учебный онлайновый курс, участие в котором открыто для всех государств — членов Организации Объединенных Наций. Цель курса — способствовать более глубокому пониманию вопросов использования информационно-коммуникационных технологий и их последствий для международной безопасности. Мы по-прежнему готовы делиться своим опытом и знаниями с государствами — членами Организации Объединенных Наций, особенно с малыми и развивающимися странами.

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

a) *Создание устойчивой к внешним воздействиям инфраструктуры*: в рамках усилий Сингапура по повышению безопасности и жизнестойкости его критически важной информационной инфраструктуры, отвечающей за оказание основных услуг, Сингапурское агентство кибербезопасности в 2019 году приступило к выполнению Генерального плана обеспечения кибербезопасности в сфере операционных технологий. В Генеральном плане, направленном на улучшение межсекторального реагирования на киберугрозы, возникающие в сфере операционных технологий, и на укрепление партнерства с промышленными кругами и другими заинтересованными сторонами, изложены основные инициативы, охватывающие людские ресурсы, процессы и технологии и нацеленные на укрепление потенциала владельцев критически важных объектов национальной информационной инфраструктуры и организаций, эксплуатирующих операционные технологические системы. В 2021 году Агентство кибербезопасности разработает и введет в действие программу регулирования производственно-сбытовых цепочек критически важной информационной инфраструктуры, предусматривающую участие заинтересованных сторон, включая правительственные учреждения, владельцев объектов критически важной информационной инфраструктуры и вендоров. В рамках этой программы всем заинтересованным сторонам будут предоставляться рекомендации по налаживанию процессов и внедрению рациональных методов управления киберрисками, угрожающими производственно-сбытовым цепочкам.

b) *Формирование более безопасного киберпространства*: в рамках наших усилий по повышению уровня национальной кибербезопасности Агентство кибербезопасности в 2020 году приступило к выполнению Генерального плана «Безопасное киберпространство», призванного: i) обеспечить защиту ключевых объектов нашей цифровой инфраструктуры; ii) обезопасить нашу деятельность в киберпространстве; iii) 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 способах защитить себя от злонамеренной киберактивности. Одной из таких инициатив является введение системы маркировки уровня кибербезопасности подключаемых к сети интеллектуальных устройств. Эта система стала внедряться в 2020 году, для начала в добровольном порядке, с тем чтобы у участников рынка и разработчиков было достаточно времени для ее опробования и осознания ее полезности. В присваиваемом устройству сертификате киберзащиты будет указываться уровень безопасности, который обеспечивается при его использовании. Ориентируясь на информацию, указанную в сертификате, потребители смогут выбирать те устройства, которые имеют наиболее высокий рейтинг с точки зрения безопасности. Данная система призвана поощрять разработку и выпуск устройств, гарантирующих более высокий уровень кибербезопасности, соответствующий общепризнанным стандартам.

c) *Развитие динамичной экосистемы кибербезопасности*: Сингапур признает, что укрепление кибербезопасности требует создания единой экосистемы кибербезопасности и поощрения инноваций в этой отрасли. Вместе с этим растет потребность в формировании резерва высококвалифицированных специалистов, которые могли бы взять на себя руководство вопросами кибербезопасности в организациях. Агентство кибербезопасности 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.

Швейцария

[Подлинный текст на английском языке]
[28 мая 2021 года]

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

Швейцария приняла ряд мер национального, регионального и глобального уровня, направленных на создание более стабильного, открытого и свободного киберпространства.

Концепция внешней политики Швейцарии на период 2020–2023 годов[3] устанавливает общие направления и приоритеты страны в области внешней политики, среди которых непрерывное участие Швейцарии в формировании открытого и безопасного цифрового пространства, основанного на международном праве и ориентированного на людей и их потребности. Швейцария также стремится укрепить позиции Женевы как ведущего глобального цифрового центра. В первой Стратегии цифровой внешней политики Швейцарии на 2021–2024 годы[4], в основу которой была положена Концепция внешней политики, закреплены ключевые принципы обеспечения открытого, свободного и безопасного цифрового пространства.

Вторая Национальная стратегия защиты Швейцарии от компьютерных рисков на 2018–2022 годы основывается на стратегических целях, изложенных в первой Национальной стратегии защиты Швейцарии от компьютерных рисков от 2012 года[5]. В обеих стратегиях признается важность информационно-коммуникационных технологий (ИКТ) как незаменимых инструментов социально-экономической и политической деятельности и закладывается основа для всеобъемлющего, интегрированного и целостного подхода к устранению угроз, связанных с использованием ИКТ. Швейцария стремится усовершенствовать раннее обнаружение киберрисков и возникающих угроз, повысить устойчивость своей критически важной инфраструктуры к внешним воздействиям и в целом снизить остроту киберугроз. Основными составляющими указанных стратегий являются необходимость формирования культуры кибербезопасности, принцип общей, но разделенной ответственности различных уровней управления и государственного и частного секторов, а также подход, основанный на оценке рисков. Они направлены на обеспечение более тесной координации на правительственном уровне и поощрение партнерства между частным и государственным секторами и более тесного сотрудничества на международной арене. Сотрудничество, будь то на национальном или международном уровне, было определено как одна из основ швейцарского подхода к борьбе с киберугрозами. В 2019 году был создан Национальный центр кибербезопасности, играющий роль контактного и координационного центра для коммерческих предприятий, научных кругов, широкой общественности и правительственных учреждений. Возглавляемый федеральным делегатом по вопросам кибербезопасности, Центр также реализует инициативы по повышению осведомленности в этой сфере.

В сентябре 2020 года Федеральный совет утвердил новую стратегию «Цифровая Швейцария»[6]. В ней определен ряд перспективных направлений сотрудничества между правительством, научными кругами, частным сектором и гражданским обществом, а ее основной целью является обеспечение цифровой трансформации швейцарского общества на благо каждого жителя страны и гарантирование всеобщей доступности открывающихся при этом возможностей.

В марте 2021 года Федеральный департамент обороны принял Стратегию кибероборонны на 2021–2024 годы[7]. Стратегия направлена на прогнозирование и раннее выявление киберугроз и злонамеренной активности, предотвращение и атрибуцию кибератак, направленных против интересов Швейцарии, обучение и

[3] URL: https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/implementing-foreign-policy/aussenpolitischestrategie.html.

[4] URL: https://www.eda.admin.ch/eda/en/fdfa/fdfa/aktuell/newsuebersicht/2020/11/digitalaussenpolitik-strategie.html.

[5] URL: https://www.ncsc.admin.ch/ncsc/en/home/strategie/strategie-ncss-2018-2022.html.

[6] URL: https://www.digitaldialog.swiss/en/.

[7] URL: www.newsd.admin.ch/newsd/message/attachments/66203.pdf.

подготовку гражданского и военного персонала, а также повышение киберустойчивости объектов критически важной инфраструктуры.

Что касается защиты объектов критически важной инфраструктуры, то Швейцария придерживается в этом плане децентрализованного подхода. Мандаты на защиту таких объектов возложены на целый ряд федеральных департаментов и управлений, таких как Федеральное управление гражданской обороны, Федеральное управление национального экономического снабжения и Федеральная разведывательная служба; таким образом, круг учреждений, ответственных за выполнение задач по киберзащите важнейших объектов, не ограничивается одним ведомством.

Принятие последовательных национальных стратегий по защите Швейцарии от киберрисков способствовало дальнейшему укреплению потенциала страны в области определения источников вредоносной активности. Для установления злоумышленников, стоящих за кибератаками, применяется целостный подход, который включает анализ технических параметров киберинцидента и учитывает геополитический контекст и в рамках которого для получения соответствующей информации задействуется весь спектр разведывательных данных. Швейцария разработала стандартизированный межведомственный процесс публичной (политической) атрибуции киберинцидентов, представляющих угрозу национальной безопасности Швейцарии. Частью проводимой в рамках этого процесса оценки является сопоставление параметров инцидента с международно-правовыми критериями юридической атрибуции киберинцидента.

В январе 2019 года в Швейцарии был создан «Кампус кибероборонны»[8]— центр прогнозирования и мониторинга потенциальных угроз, возникающих в результате развития технологий, на базе которого разрабатываются методы снижения риска и ведется подготовка экспертов в области кибербезопасности. «Кампус» объединяет экспертов из Федерального управления закупок для оборонного комплекса, а также представителей промышленности и сотрудников научно-исследовательских организаций.

Что касается информационно-просветительской деятельности и взаимодействия с частным сектором и научными кругами, то Швейцария поощряет самые разные инициативы в этом направлении. Например, в целях противодействия шпионажу и деятельности, которая может привести к распространению оружия массового уничтожения, Федеральная разведывательная служба с 2004 года осуществляет кампанию по превентивному информированию «Профилакс», в рамках которой предприятиям, университетам и научно-исследовательским учреждениям предоставляются консультации по вопросам упреждающего обнаружения и пресечения незаконной деятельности по шпионажу и распространению.

Содержание концепций, упомянутых в докладах Группы правительственных экспертов

В приложении к оценке угроз следует отметить, что злонамеренная киберактивность, нацеленная непосредственно на объекты критически важной инфраструктуры, может нанести серьезный ущерб и отрицательно повлиять на функционирование основных служб, в частности в сфере здравоохранения. За последние годы несколько швейцарских федеральных ведомств и частных компаний стали жертвами злонамеренной киберактивности (кибершпионажа), спонсируемой государствами. Конечной целью этой злонамеренной

[8] URL: www.ar.admin.ch/en/armasuisse-wissenschaft-und-technologie-w-t/cyber-defence_campus.html.

кибератаки, как правило, является получение экономических, политических и военных преимуществ. В течение 2020 года объекты критически важной инфраструктуры Швейцарии пострадали в основном от атак, мотивированных получением финансовой выгоды. В будущем Швейцария ожидает увеличения числа атак с использованием вирусов-вымогателей, осуществляемых преступными группами, а также кибероперациий, проводимых и спонсируемых государствами или осуществляемых с попустительства государств. Кроме того, злонамеренная кибератаки может иметь непреднамеренные последствия для Швейцарии и повлечь за собой сопутствующий ущерб. Поскольку субъекты угроз продолжают разрабатывать методы и инструменты для выведения из строя легитимного программного обеспечения и перехвата контроля над им, особое беспокойство вызывают атаки на производственно-сбытовые цепочки.

Швейцария активно участвовала в работе шестой Группы правительственных экспертов (2019–2021 годы) и Рабочей группы открытого состава (2019–2021 годы) и внесла вклад в рассмотрение ими вопросов, касающихся международной стабильности в киберпространстве и укрепления осуществления принципов ответственного поведения государств в киберпространстве Организации Объединенных Наций. Швейцария убеждена, что ключом к обеспечению и поддержанию международной кибербезопасности являются применение международного права, включая право прав человека и международное гуманитарное право, соблюдение добровольных необязательных норм, принятие мер по укреплению доверия и наращивание потенциала. Председателем Рабочей группы открытого состава выступал Постоянный представитель Швейцарии при Организации Объединенных Наций в Нью-Йорке. Именно под его председательством Группа в марте 2021 года согласовала свой консенсусный итоговый доклад (A/75/816).

Стремясь обеспечить координацию с другими процессами в рамках Организации Объединенных Наций, Швейцария сотрудничает с Международным союзом электросвязи, в частности в рамках консультаций по основным принципам использования Глобальной программы кибербезопасности.

Швейцария стремится укрепить роль Организации по безопасности и сотрудничеству в Европе (ОБСЕ) в обеспечении стабильности в киберпространстве и активно участвует в работе ее неофициальной рабочей группы по вопросам кибербезопасности. После утверждения мандата ОБСЕ на разработку и осуществление мер по укреплению доверия Швейцария предприняла ряд шагов для повышения прозрачности в отношении позиции, занимаемой ею по вопросам киберпространства; так, она обменивается информацией о национальных структурах и организациях, занимающихся вопросами кибербезопасности, и о своей соответствующей политике в ходе регулярных заседаний неофициальных рабочих групп, через поддерживаемые ОБСЕ платформы и через Коммуникационную сеть ОБСЕ. Кроме того, совместно с Германией Швейцария продолжает работать над введением в действие информационно-консультативного механизма, предусмотренного мерой по укреплению доверия № 3.

Швейцария является государством — участником Конвенции Совета Европы о киберпреступности и считает, что ее имплементация и практическое применение закрепленных в ней принципов имеют решающее значение для эффективной борьбы с киберпреступностью. Швейцария участвует в переговорах по второму дополнительному протоколу к Конвенции, который направлен на укрепление международного сотрудничества.

На двустороннем уровне Швейцария проводит со странами регулярные политические консультации по вопросам, касающимся киберпространства.

В 2019 году Швейцария присоединилась к Коалиции за свободу в Интернете, став ее тридцать первым членом. Швейцария твердо убеждена в том, что права, которыми люди пользуются в обычной жизни, должны быть защищены и при пользовании Интернетом. Коалиция за свободу в Интернете — это одна из ключевых инициатив по укреплению взаимодействия между всеми заинтересованными сторонами в целях защиты прав человека и основных свобод в эпоху Интернета. Помимо прочей помощи Швейцария оказывает Коалиции за свободу в Интернете также и финансовую поддержку.

В 2019 году Швейцария инициировала серию экспертных юридических диалогов по вопросам применения международного права в киберпространстве. В 2021 году Швейцария продолжит эти усилия в целях содействия достижению общего понимания в отношении того, как следует применять международное право, с акцентом на порядок применения международного гуманитарного права в киберпространстве.

В 2018 году Швейцария положила начало Женевскому диалогу по вопросам ответственного поведения в киберпространстве, который представляет собой многостороннюю платформу для обсуждения ролей и обязанностей, касающихся поддержания международной стабильности в киберпространстве. С 2020 года особое внимание в рамках Женевского диалога уделяется роли коммерческих предприятий в реализации норм, согласованных на международном уровне.

Недавно Национальный центр кибербезопасности инициировал межведомственный процесс, направленный на выработку общегосударственного подхода к скоординированному и ответственному раскрытию новейших уязвимостей в киберпространстве. Этот процесс позволяет исследователям, обнаружившим какой-либо фактор уязвимости в аппаратном или программном обеспечении или в цифровых услугах, сообщить о находке экспертам Центра. Раскрытие информации направлено на снижение уязвимости (например, путем выпуска патчей) до того, как она будет использована в злонамеренных целях.

Швейцария участвует в ряде национальных и международных учений, направленных на тестирование национального потенциала, процедур и процессов принятия решений, в частности в учениях «Сомкнутые щиты».

Швейцария является одним из членов –– основателей Глобального форума по обмену опытом в области компьютерных технологий и поддерживает различные проекты по наращиванию киберпотенциала. Кроме того, Швейцария финансово поддерживает инициативы, направленные на укрепление способности дипломатов и представителей неправительственных организаций участвовать в соответствующих процессах, связанных с обеспечением международной кибер-стабильности, на уровне Организации Объединенных Наций и вносить в них конструктивный вклад.

Турция

[Подлинный текст на английском языке]
[31 мая 2021 года]

Информационно-коммуникационные технологии (ИКТ) прочно вошли в социально-экономическую жизнь общества. Эти технологии используются в самых различных сферах, охватывающих деятельность государственного и частного секторов, важнейшие объекты инфраструктуры и отдельных людей, и получили широкое распространение в Турции и во всем мире. В результате этого ИКТ играют важную роль в достижении устойчивого роста и развития. Однако

чем более активно мы используем технологии, тем в бóльшую зависимость от них мы попадаем и тем более уязвимыми мы становимся по отношению к рискам, сопряженным с их использованием. Физические лица, компании, объекты критически важной инфраструктуры и государства — все они сталкиваются с серьезными проблемами, создаваемыми киберугрозами.

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. Что касается национальной стратегии и плана действий в области кибербезопасности на период 2020–2023 годов, то в их разработке участвовали все соответствующие заинтересованные стороны, работавшие по линии профильных аналитических групп под координирующим руководством Министерства транспорта и инфраструктуры.

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

- защита объектов критически важной инфраструктуры и повышение устойчивости к внешним воздействиям;
- наращивание национального потенциала;
- создание органической сети кибербезопасности;
- обеспечение безопасности технологий нового поколения (Интернет вещей, сеть 5G, облачные технологии и т. д.);
- борьба с киберпреступностью;
- развитие и поддержка местных и общенациональных технологий;
- интеграция аспектов кибербезопасности в систему национальной безопасности;
- расширение международного сотрудничества.

Кроме того, с 2013 года проводимую в Турции работу по реагированию на инциденты в цифровом пространстве координирует Национальная группа реагирования на инциденты в области кибербезопасности, входящая в состав Управления информационно-коммуникационных технологий. Помимо выявления киберугроз и реагирования на инциденты в киберпространстве, 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 связанными с кибербезопасностью направлениями деятельности Национальной группы реагирования на инциденты в области кибербезопасности являются:

- наращивание киберпотенциала;
- принятие мер технического характера;
- сбор и распространение информации об угрозах;

- защита объектов критически важной инфраструктуры.

В 2013 году в рамках работы по укреплению национальной кибербезопасности было создано 14 секторальных групп реагирования на инциденты в области кибербезопасности, обслуживающих объекты критически важной инфраструктуры и важнейшие секторы (такие как энергетика, здравоохранение, банковское дело и финансы, управление водными ресурсами, электронные коммуникации и важнейшие государственные услуги), и 1803 группы учрежденческого уровня. В целях смягчения киберрисков и борьбы с киберугрозами все эти группы, координируемые национальной командой экспертов по кибербезопасности, работают круглосуточно и без выходных. Национальная группа реагирования на инциденты в области кибербезопасности располагает арсеналом инструментов обнаружения и предупреждения, которые она использует для целей мониторинга, а также инструментов отчетности, применяемых для обмена информацией с соответствующими сторонами. Она разработала платформу, с помощью которой все действующие в Турции группы реагирования на чрезвычайные ситуации в киберпространстве могут обмениваться информацией, в частности передавать сигналы тревоги, предупреждения и оповещения, касающиеся безопасности, что обеспечивает эффективный и безопасный канал связи.

Национальная группа реагирования на инциденты в области кибербезопасности организует и помогает проводить учебные курсы, летние тематические лагеря и конкурсы по кибербезопасности, участие в которых открыто для ряда сообществ. Кроме того, Национальная группа проводит для других групп реагирования на инциденты в области кибербезопасности учебные занятия по таким темам, как анализ вредоносных программ и анализ журналов регистрации событий. За последние четыре года в организованных Национальной группой учебных занятиях, посвященных различным аспектам кибербезопасности, приняли участие более 5000 человек.

Кроме того, в целях наращивания резерва высококвалифицированных профильных кадров Академия кибербезопасности, действующая при Управлении информационно-коммуникационных технологий, проводит открытые онлайновые занятия по кибербезопасности и другим смежным областям. Материалы учебных занятий доступны на официальном веб-сайте Академии (www.btkakademi.gov.tr/portal).

Помимо этого, ряд турецких организаций, учреждений, университетов, неправительственных организаций и структур частного сектора также проводят по всей стране семинары, конференции и учебные занятия по вопросам кибербезопасности, защиты объектов критически важной инфраструктуры и другим смежным темам.

К числу мероприятий по повышению осведомленности относится ежегодный День безопасного Интернета, главная цель которого — поощрять сознательное и безопасное пользование Интернетом. На официальном веб-портале «Безопасный Интернет» (www.guvenlinet.org.tr/) в открытом доступе размещены ссылки на веб-сайт «Безопасность в сети» и на горячую линию по вопросам безопасности в Интернете, при помощи которых семьи могут получить советы и рекомендации по эффективному использованию Всемирной сети.

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

Атаки вредоносных программ, фишинговые атаки и другие киберугрозы, активизировавшиеся на фоне пандемии COVID-19, анализируются Национальной группой реагирования на инциденты в области кибербезопасности, которая работает круглосуточно и без выходных. Входящие в структуру Национальной группы центры управления и контроля выявляют и блокируют вредоносные цепочки киберугроз, тем самым обеспечивая защиту критически важной инфраструктуры и граждан. При этом составляются отчеты о киберугрозах, которые распространяются среди соответствующих сторон. 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.

Турция играет важную роль во многих организациях, занимающихся вопросами кибернетической и информационной безопасности, либо являясь одним из их членов-основателей, либо содействуя их совместной работе в этой сфере. Турция придает большое значение обмену информацией по широкому кругу вопросов с различными странами и организациями. Национальная группа реагирования на инциденты в области кибербезопасности является членом следующих структур: Форум групп оперативного реагирования и обеспечения безопасности, организация «Доверенные инициаторы», Международный союз электросвязи (МСЭ), Многонациональная программа Организации Североатлантического договора (НАТО) по обмену информацией о вредоносных программах, Альянс по кибербезопасности для взаимного прогресса и Группа реагирования на инциденты в области кибербезопасности Организации Исламская конференция. Кроме того, с ноября 2015 года Турция в качестве страны-спонсора принимает участие в работе Центра передового опыта НАТО по совместной киберзащите. Продолжается также двустороннее и многостороннее сотрудничество по вопросам кибербезопасности со многими странами, в частности в форме подписания меморандумов о взаимопонимании. К тому же Турция активно участвует 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, Совет сотрудничества тюркоязычных государств и Региональный центр по содействию проверке и осуществлению контроля над вооружениями — Центр по сотрудничеству в сфере безопасности.

Еще одним важным элементом укрепления сотрудничества и обеспечения готовности является проведение учений по кибербезопасности. Такие учения, проводимые на национальном и международном уровнях, способствуют повышению безопасности в киберпространстве и помогают отработать меры противодействия потенциальным киберугрозам. Начиная с 2011 года Министерство транспорта и инфраструктуры четыре раза организовывало учения по кибербезопасности на национальном уровне и два раза — на международном. Последние на сегодняшний день учения — международные учения по кибербезопасности «Киберщит-2019», совместно организованные Министерством транспорта и инфраструктуры и Управлением информационно-коммуникационных технологий, — были проведены 19 декабря 2019 года в Анкаре. Поддержку в проведении этих учений оказали МСЭ и Альянс по кибербезопасности для взаимного прогресса. Кроме того, Турция участвует в целом ряде международных учений по кибербезопасности, таких как «Сомкнутые щиты НАТО», «Киберкоалиция

НАТО» и учения НАТО по урегулированию кризисов, а также вносит вклад в организацию этих мероприятий. 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 киберинциденты во всем мире.

Обеспечение международного мира и безопасности в киберпространстве требует проведения дальнейших исследований, в основе которых должно лежать расширенное международное сотрудничество. Совершенно очевидно, что соблюдение принципов международного права, а также норм и правил, изложенных в докладах групп правительственных экспертов и рабочих групп открытого состава и в других соответствующих аналитических материалах, будет способствовать укреплению безопасности в киберпространстве.

Кроме того, важными компонентами борьбы с киберугрозами являются укрепление сотрудничества и поддержка механизмов обмена информацией, и соответствующей работе следует уделять должное внимание.

Следует также отметить, что Турция осознает важность соблюдения международного права и норм ответственного поведения государств в киберпространстве и признает необходимость эффективного международного сотрудничества в этой сфере. Турция принимает энергичные меры для достижения данных целей и подчеркивает, что укрепление кибербезопасности на национальном и международном уровнях будет оставаться одним из ее ключевых приоритетов.

Украина

[Подлинный текст на английском языке]
[31 мая 2021 года]

Анализ имеющейся информации показывает, что в условиях «гибридной» войны против нашего государства одной из главных угроз национальной безопасности являются осуществляемые Российской Федерацией деструктивные информационно-психологические спецоперации, направленные на подрыв конституционного строя, нарушение суверенитета и территориальной целостности Украины, а также на обострение общественно-политической и социально-экономической ситуации в нашей стране. Целенаправленное распространение дезинформации и сфабрикованной информации, наряду с вооруженной агрессией, превратилось в насущную угрозу не только для Украины, но и для всего мира, поскольку такая информация влияет на сознание граждан других стран, создает искаженный образ Украины и формирует общественное мнение, выгодное исключительно России.

Государство-агрессор все чаще принимает меры, направленные на снижение уровня информационной безопасности нашего государства, создает рычаги влияния на государственные институты и информационное пространство в целях укрепления собственных позиций, формирования благоприятного мнения о себе за рубежом и оказания давления на государственные институты Украины для принятия решений в свою пользу. Для этого в украинском информационном и медиапространстве, а также в Интернете на систематической основе ведется пропаганда, в том числе через социальные сети, программы мгновенного обмена сообщениями, электронные ресурсы и специально разработанные информационные продукты, в особенности дезинформирующего характера.

Для оказания этого негативного информационного воздействия на нашу страну в Российской Федерации создана мощная система распространения пропагандистских материалов, которая включает сеть информационных платформ (блоги, веб-сайты), контролируемые средства массовые информации и интернет-ресурсы, сайты-агрегаторы и новостные сайты, блогеров и лидеров мнений, публикующих соответствующие материалы, информационные агентства, а также компании, оказывающие услуги в области связей с общественностью, и позволяет размещать пропагандистские сообщения на ведущих новостных лентах. Кроме того, для быстрого распространения ложных сведений и антиукраинских сообщений, предназначенных для манипуляции массовым сознанием, Россия широко использует бот-сети. Основными субъектами информационного пространства, используемыми российской стороной для распространения ложных сведений, являются ведущие мировые социальные сети («Фейсбук», «Инстаграм», «Твиттер»), аудитория которых стремительно расширилась ввиду закрытия в Украине доступа к российским социальным сетям «ВКонтакте» и «Одноклассники». Согласно наблюдаемой тенденции, пользователей украинского сегмента Интернета переориентируют на широкое использование служб обмена сообщениями («Телеграм», «Уотсапп», «Вайбер» и др.) из-за возможности сохранения анонимности, удобства размещения и дальнейшего массового распространения материалов, а также высокой степени интерактивности и оперативной обратной связи.

Помимо этого, для распространения дезинформации используются видеохостинги «Ютуб», «Яндекс.Видео», «Рутуб», «Видео@Mail.Ru»), поскольку компании, владеющие фото- и видеохостингами, действуют в соответствии с законодательством стран, на территории которых они расположены. Российские пропагандисты пользуются данным обстоятельством, создавая и размещая на этих веб-платформах материалы, представляющие угрозу информационной безопасности Украины. Ввиду того, что источником таких сообщений являются американские и европейские хостинги, эти материалы свободно распространяются в Интернете.

Помимо этого страна-агрессор прилагает усилия для постоянного развития сети подконтрольных ей информационных ресурсов. В частности, оккупационные администрации на временно оккупированных территориях нашего государства принимают систематические меры по созданию новых информационных платформ, увеличению количества телевизионных каналов и расширению зоны охвата телерадиовещания, в том числе на территориях, подконтрольных украинским властям. Помимо распространения антиукраинских материалов, российские оккупационные власти подавляют сигнал отечественного телерадиовещания при помощи мощного ретрансляционного оборудования, генерирующего так называемый «белый шум» на частотах, которые используются украинской стороной для донесения объективной информации до жителей временно оккупированных территорий. Это особенно важно с учетом использования крупнейшими медиагруппами страны («Интер Медиа Груп», «СтарЛайтМедиа», «Медиа Группа Украина», «1+1») на своих телеканалах кодированного спутникового сигнала, а также на фоне неудовлетворительного уровня охвата территории Украины национальным цифровым телерадиовещанием. В результате жители приграничных районов Украины находятся под постоянным воздействием деструктивной информации, транслируемой основными пропагандистскими каналами Российской Федерации. Еще одним фактором негативного влияния, мешающим донести до жителей временно оккупированных территорий Украины информацию оппозиционного характера, является деятельность операторов и поставщиков услуг связи на временно оккупированных территориях, направленная на ограничение доступа местного населения к украинскому сегменту

Интернета. Так, в нарушение европейского законодательства, регистрацией IP-адресов для работы так называемых поставщиков интернет-услуг в Крыму и оккупированных районах Донбасса занимается некоммерческая организация RIPE NCC (Нидерланды). В целях приведения деятельности этой организации в соответствие с действующим законодательством Украины Министерство иностранных дел Украины и Посольство Украины в Королевстве Нидерландов принимают соответствующие меры на межгосударственном уровне.

Кроме того, известны случаи использования Российской Федерацией сервисов, принадлежащих компаниям «Эппл» и «Гугл», для распространения дезинформации в целях манипулирования пользователями украинского сегмента Интернета. В частности, в магазинах «Эпп стор» и «Плей маркет» представлены мобильные приложения, разработанные юридическими и физическими лицами, в отношении которых действуют специальные экономические и другие ограничительные меры (санкции), введенные в соответствии с решением Совета национальной безопасности и обороны от 14 мая 2020 года о применении, отмене и внесении изменений в персональные специальные экономические и другие ограничительные меры (санкции), введенным в действие Указом Президента Украины от 14 мая 2020 года № 184/2020. Функционал данных программных продуктов предусматривает техническую возможность обеспечения доступа к запрещенным в Украине веб-ресурсам.

Несмотря на все усилия нашего государства по укреплению информационной безопасности и блокированию распространения ложных сведений как одной из наиболее существенных угроз в информационной сфере, крайне необходимо помочь мировому сообществу и международным институтам оказать надлежащее противодействие информационной агрессии со стороны Российской Федерации в отношении не только Украины, но и других стран, с позиций которых она осуществляет деструктивное воздействие в информационном пространстве.

До недавнего времени деструктивное информационное воздействие со стороны Российской Федерации, ее попытки вмешательства во внутренние дела нашего государства и навязывания своих условий в рамках международного сотрудничества и внутренних процессов осуществлялись через аффилированные украинские политические партии и движения, тайное прямое финансирование гражданских институтов и хозяйствующих субъектов, действующих на территории нашего государства, силовое давление посредством военной агрессии на востоке Украины и блокирования международной поддержки Украины и ее вступления в Европейский союз и Организацию Североатлантического договора (НАТО), проведение информационных кампаний, операций и акций при помощи контролируемых информационных ресурсов.

Вместе с тем наблюдается устойчивая тенденция, которая проявляется в том, что Российская Федерация переориентирует свою дальнейшую стратегию так называемой «информационной войны» с Украиной, все чаще скрывая свое участие в организации и проведении деструктивных мероприятий, направленных против нашего государства, путем осуществления их с площадок так называемых «третьих» стран. С одной стороны, это обусловлено экономическими санкциями, введенными Европейским союзом и Соединенными Штатами в отношении Российской Федерации за вмешательство во внутренние дела Украины, аннексию Автономной Республики Крым и развязывание вооруженного конфликта на временно оккупированных территориях Донецкой и Луганской областей. С другой стороны, это обусловлено также мерами, принимаемыми украинской стороной для борьбы с деструктивным влиянием страны-агрессора на украинское информационное пространство и сознание граждан, смягчения негативных последствий распространения соответствующих сообщений и

повышения уровня патриотизма, а также укрепления самосознания населения нашего государства.

В частности, участились акции информационного воздействия и случаи вмешательства во внутренние дела Украины. Российская Федерация ведет разведывательную и подрывную деятельность с площадок государств — членов НАТО и Европейского союза, которая заключается в создании и финансировании лоббистов российских интересов в общегосударственных и местных органах власти, политических партиях и движениях, экспертном и блогерском сообществе, аналитических центрах, рекламных и консалтинговых компаниях, среди субъектов, занимающихся благотворительностью, неправительственных организаций и лидеров общественного мнения, а также в создании контролируемых средств массовой информации, интернет-ресурсов и компаний, оказывающих услуги в области связей с общественностью.

Благодаря пособничеству пророссийских европейских политиков — представителей так называемых ячеек «русского мира» в Евросоюзе — Российская Федерация пытается легализовать и навязать мировому сообществу идею легитимности крымского плебисцита, оправдать вооруженную агрессию, осуществляемую ею в отношении Украины и, соответственно, добиться отмены антироссийских санкций и своего возвращения в мировой политический истеблишмент. В настоящее время в некоторых европейских государствах действуют пророссийские субъекты. Большинство представителей этих политических сил, лоббируя интересы страны-агрессора как внутри, так и за пределами своей страны, пропагандируют пророссийские взгляды, распространяют российскую версию происходящих событий и проводят информационную работу, которая несет угрозу национальным интересам Украины.

Переход Российской Федерации к практике организации и проведения информационных спецопераций и акций деструктивного информационного воздействия с позиций «третьих» стран выражается в том, что она подогревает исторические разногласия и инспирирует территориальные претензии других государств к Украине, а также провоцирует сепаратистские и автономные проявления со стороны национальных меньшинств в Украине. С одной стороны, это осложняет отношения нашего государства с соседними странами, с площадок которых Российская Федерация осуществляет такую разрушительную деятельность, а с другой — служит для этих стран поводом заявить о своих территориальных претензиях на определенную часть украинских земель. В то же время, официально дистанцируясь от этого процесса, Россия избегает прямых обвинений со стороны Украины и мирового сообщества во вмешательстве во внутренние дела нашего государства, а также создает непосредственную угрозу для добрососедских отношений Украины с другими государствами, с тем чтобы создать позиции влияния на внутриполитическую ситуацию в Украине.

Учитывая вышесказанное, Украина продолжит принимать комплексные меры по обеспечению ответственного поведения в киберпространстве в контексте международной безопасности, одновременно призывая к поддержке со стороны мирового сообщества и к оказанию совместными усилиями надлежащего противодействия «гибридной» войне, развязанной Российской Федерацией.

Чтобы обеспечить осуществление реформы законодательства об электронной цифровой подписи путем его согласования с положениями регламента (ЕС) № 910/2014 Европейского парламента и Совета Европейского союза от 23 июля 2014 года об электронной идентификации и доверительных услугах для осуществления электронных трансакций на внутреннем рынке и об отмене Директивы 1999/93/ЕС Европейского парламента и Совета, Верховная Рада Украины

5 октября 2017 года приняла Закон № 2155-VIII об электронных доверительных услугах, который вступил в силу 7 ноября 2018 года.

Основная цель заключается в том, чтобы внедрить в Украине модели и принципы предоставления электронных доверительных услуг, используемые в Европейском союзе, не разрушая при этом сложившуюся в Украине систему взаимодействия сторон в сфере использования электронной цифровой подписи. В упомянутом выше законе определяются правовые и организационные принципы предоставления электронных доверительных услуг, в том числе трансграничных, права и обязанности субъектов правовых отношений в сфере электронных доверительных услуг, порядок осуществления государственного надзора (контроля) за соблюдением требований законодательства в сфере электронных доверительных услуг, а также правовые и организационные принципы осуществления электронной идентификации. В развитие положений Закона № 2155-VIII Кабинет министров Украины принял ряд постановлений:

- № 749 об утверждении порядка использования электронных доверительных услуг в органах государственной власти, органах местного самоуправления, предприятиях, учреждениях и организациях государственной формы собственности, принятое Кабинетом министров Украины 19 сентября 2018 года;
- № 775 об утверждении обязательных требований к Доверительному списку, принятое Кабинетом министров Украины 26 сентября 2018 года;
- № 821 об утверждении порядка хранения документированной информации и ее передачи центральному заверительному органу в случае прекращения деятельности квалифицированного поставщика электронных доверительных услуг, принятое Кабинетом министров Украины 10 октября 2018 года;
- № 992 об утверждении требований в сфере электронных доверительных услуг и порядка проверки соблюдения требований законодательства в сфере электронных доверительных услуг, принятое Кабинетом министров Украины 7 ноября 2018 года;
- № 1215 об утверждении порядка проведения процедуры оценки соответствия в сфере электронных доверительных услуг, принятое Кабинетом министров Украины 18 декабря 2018 года;
- № 60 об утверждении порядка взаимного признания украинских и иностранных сертификатов открытых ключей, электронных подписей, а также использования информационно-телекоммуникационной системы центрального заверительного органа для обеспечения признания в Украине электронных доверительных услуг, иностранных сертификатов открытых ключей, используемых при предоставлении юридически значимых электронных услуг в процессе взаимодействия между субъектами различных государств, принятое Кабинетом министров Украины 23 января 2019 года.

Администрация Государственной службы специальной связи и защиты информации Украины во исполнение требований статьи 8 вышеуказанного закона приказом от 14 мая 2020 года утвердила требования по обеспечению безопасности и защиты информации о квалифицированных поставщиках электронных доверительных услуг и их отдельных пунктах регистрации (приказ зарегистрирован в Министерстве юстиции Украины 16 июля 2020 года); в этом документе подробно изложен и определен порядок соблюдения вышеупомянутого закона и требований в сфере электронных доверительных услуг, утвержденных Кабинетом министров Украины 7 ноября 2018 года в постановлении № 992, с целью

обеспечить безопасность и защиту информации о поставщиках электронных доверительных услуг и отдельных пунктах регистрации.

В настоящее время Украина принимает меры, направленные на обеспечение взаимного признания электронных доверительных услуг в рамках Соглашения об ассоциации между Украиной и Европейским союзом и по итогам договоренностей, достигнутых между Украиной и Европейским союзом в ходе двадцать второго саммита Европейский союз — Украина.

Вместе с тем некоторые положения вышеупомянутого закона необходимо пересмотреть, чтобы привести их в максимальное соответствие с положениями регламента (ЕС) № 910/2014, прежде всего в части установления принципов государственного регулирования в сфере электронной идентификации, требований к усовершенствованным электронным подписям и печатям, а также уточнения требований к квалифицированным электронным подписям и печатям. Законопроект, подготовленный Министерством цифровой трансформации и Администрацией Государственной службы специальной связи и защиты информации Украины, в настоящее время находится на рассмотрении Кабинета министров Украины.

Кроме того, постановлением № 24 от 13 января 2021 года Кабинет министров Украины внес изменения в пункт 4 Положения об Администрации Государственной службы специальной связи и защиты информации Украины, в котором говорится о задачах данной структуры, закрепив за ней функции Органа по аккредитации в области безопасности в соответствии со статьей 7 Административных договоренностей по охране информации с ограниченным доступом между Правительством Украины и Организацией Североатлантического договора (НАТО), ратифицированных Законом № 2068 от 24 мая 2017 года.

Администрация Государственной службы специальной связи и защиты информации Украины, утвердив национальную процедуру аккредитации в области безопасности коммуникационно-информационных систем, в которых осуществляется обмен информацией НАТО с ограниченным доступом, принимает меры в целях выполнения нормативных требований НАТО, касающихся данных вопросов.

В рамках развития международного сотрудничества и повышения осведомленности специалистов по информационной безопасности Администрация Государственной службы специальной связи и защиты информации Украины участвует в международных конференциях Механизма технической помощи и обмена информацией Европейской комиссии (Technical Assistance and Information Exchange Instrument of the European Commission, TAEIX) и семинарах, проводимых компанией «ФаерАй».

В целях укрепления информационной безопасности ведется непрерывная работа по внедрению системы аудита информационной безопасности на объектах критически важной инфраструктуры, заключающаяся в следующем:

- формирование требований к независимым специалистам по аудиту информационной безопасности на объектах критической инфраструктуры;
- разработка процедуры аттестации/переаттестации специалистов по аудиту информационной безопасности, а также разработка системы целевой оценки профессиональной подготовки специалистов по аудиту информационной безопасности и анализа результатов независимого аудита информационной безопасности информационно-телекоммуникационных сетей как объектов критической инфраструктуры;

Вместе с тем в целях реализации государственной политики в сфере защиты информации сотрудники Администрации Государственной службы специальной связи и защиты информации Украины проводят на национальном уровне мероприятия по контролю за поддержанием предусмотренного законодательством уровня технической защиты государственных информационных ресурсов и информации в киберпространстве.

Кроме того, в целях подготовки и обеспечения принятия нижеперечисленных актов Администрация Государственной службы специальной связи и защиты информации Украины предприняла следующие действия:

– подготовила подробные предложения по проекту стратегии кибербезопасности Украины (2021–2025 годы) в соответствии со статьей 107 Конституции Украины, частью второй статьи 2 закона об основах национальной безопасности и Указом Президента Украины № 391/2020 о решении Совета национальной безопасности и обороны от 14 сентября 2020 года;

– содействовала принятию постановления Кабинета министров Украины № 518 от 19 июня 2019 года об утверждении общих требований к киберзащите критической инфраструктуры, инициированного в рамках формирования и реализации государственной политики в области киберзащиты критической информационной инфраструктуры и направленного на обеспечение совместимости с соответствующими стандартами Европейского союза и НАТО, а также на создание нормативно-терминологической базы по кибербезопасности и гармонизацию нормативных актов в сфере информационной безопасности и кибербезопасности в соответствии с международными стандартами;

– Кабинет министров Украины принял постановление № 1109 о некоторых вопросах объектов критической инфраструктуры и постановление № 943 о некоторых вопросах объектов критической информационной инфраструктуры; эти постановления были подготовлены с учетом требований законодательства Европейского союза, в частности директивы (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года о мерах по достижению высокого общего уровня безопасности сетевых и информационных систем Союза и директивы Совета 2008/114/ЕС от 8 декабря 2008 года об определении и обозначении европейской критической инфраструктуры и оценке необходимости усиления ее защиты;

– 11 ноября 2020 года Кабинет министров Украины принял постановление № 1176 об утверждении порядка проведения обзора состояния киберзащиты критической информационной инфраструктуры, государственных информационных ресурсов и информации, необходимость защиты которых предусмотрена законодательством; утвержденный документ позволяет регулировать вопросы, связанные с информационной инфраструктурой, государственными информационными ресурсами и информацией, требование относительно защиты которых установлено законом.

Группа реагирования на компьютерные инциденты Украины постоянно проводит мероприятия в рамках сотрудничества с аналогичными группами за рубежом в целях решения вопросов преодоления последствий кибератак на объекты критической информационной инфраструктуры, анализирует данные об инцидентах в области кибертехнологий, предоставляет владельцам объектов кибербезопасности практическую помощь в предотвращении и выявлении инцидентов в области кибертехнологий и ликвидации последствий, подготавливает и публикует на своем официальном веб-сайте рекомендации по борьбе с

современными видами кибератак и киберугроз, а также информирует о киберугрозах и надлежащих методах защиты от них.

Соединенное Королевство Великобритании и Северной Ирландии

[Подлинный текст на английском языке]
[31 мая 2021 года]

Соединенное Королевство с удовлетворением отмечает предложение проинформировать Генерального секретаря о своей точке зрения и об оценках по вопросам, касающимся поощрения ответственного поведения государств в киберпространстве в контексте международной безопасности, о чем подробно говорится в резолюции 75/32 Генеральной Ассамблеи. Мы призываем все государства, участвующие в обсуждениях достижений в сфере информатизации и телекоммуникаций в контексте международной безопасности, воспользоваться этой и последующими возможностями.

В киберпространстве государственные границы не имеют значения. Будучи ответственной кибердержавой, Соединенное Королевство намерено работать над формированием будущих рамок регулирования киберпространства, придерживаясь действующих правил и добиваясь консенсуса в отношении позитивных норм поведения в сегодняшнем мире, где технологии играют основополагающую роль.

Соединенное Королевство признает, что в предстоящее десятилетие человеческое общество примет иной облик в результате стремительных технологических преобразований в таких областях, как искусственный интеллект, кибернетика и работа с данными. Страны должны работать сообща в интересах решения наиболее важных глобальных проблем, и в частности в целях содействия формированию свободного, открытого, мирного и безопасного киберпространства, и нести миру добро, защищая демократию и права человека в условиях цифровизации общества.

Мы будем способствовать внедрению и соблюдению этих правил и норм и будем вести совместную работу со всем спектром партнеров и заинтересованных сторон, чтобы убедительно доказать необходимость создания такого киберпространства, в котором открытость общества была бы под защитой и обеспечивались бы инновации, развитие и экономический рост. Кроме того, занимаясь наращиванием потенциала на международном уровне, мы будем поддерживать страны, испытывающие трудности в сфере цифровизации, чтобы придать им больше уверенности в своих силах для участия в международных дискуссиях и расширения возможностей в сфере кибербезопасности.

Соединенное Королевство с удовлетворением отмечает успешное завершение таких параллельных процессов Организации Объединенных Наций, как деятельность Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и работа Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности. Деятельность Рабочей группы открытого состава стала инклюзивным процессом, в рамках которого удалось собрать различные мнения всех государств-членов и других заинтересованных сторон, а доклад Группы правительственных экспертов, по нашему мнению, станет подробным руководством по разработке первоначальных принципов ответственного поведения государств в киберпространстве, в чем заинтересованы многие государства.

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

16 марта 2021 года правительство Соединенного Королевства опубликовало документ под названием *Global Britain in a competitive age. The Integrated Review of Security, Defence, Development and Foreign Policy* («Место Британии в глобальных процессах в эпоху конкуренции. Комплексный обзор вопросов безопасности, обороны, развития и внешней политики»)[9], в котором изложило свое видение той роли, которую Соединенное Королевство будет играть в мире на протяжении следующего десятилетия, а также те шаги, которые страна намерена предпринять до 2025 года. В этом обзоре отмечается необходимость формирования международного порядка с учетом будущих последствий развития кибертехнологий и космических технологий, благодаря которым стремительно ширятся возможности для экономической, социальной и военной деятельности. Мы будем прилагать активные усилия по обеспечению эффективной подотчетности и надзора, который позволит защищать идеалы демократии, одновременно выступая против чрезмерного государственного регулирования.

Кроме того, в 2021 году Великобритания намерена принять новую комплексную киберстратегию, которая придет на смену предыдущей национальной стратегии кибербезопасности на период 2016–2021 годов. В основе новой стратегии будет лежать необходимость общегосударственного подхода к проблемам в сфере кибертехнологий, что согласуется с выводами, сделанными по итогам комплексного обзора. В рамках этой стратегии мы ставим перед собой следующие первоочередные задачи:

- укрепить киберэкосистему Соединенного Королевства, обеспечивая общегосударственный подход к вопросам кибертехнологий и развивая партнерские отношения между правительством, научными кругами и промышленностью;
- построить устойчивое к внешним воздействиям и процветающее цифровое Соединенное Королевство, в котором граждане смогут чувствовать себя в безопасности, находясь в интернет-пространстве, и быть уверенными в том, что их данные защищены;
- занять лидирующие позиции в сфере развития технологий, жизненно важных для кибердержавы, таких как микропроцессоры, защищенные системы, квантовые технологии и новые формы передачи данных;
- поощрять формирование свободного, открытого, мирного и безопасного киберпространства, сотрудничая с правительствами других стран и промышленными кругами и опираясь на ведущую роль Соединенного Королевства как генератора идей в сфере кибербезопасности;
- выявлять противников нашего государства, пресекать их деятельность и препятствовать совершению ими враждебных действий.

В рамках усилий по решению этих задач совместно с другими правительствами и в партнерстве с промышленными кругами мы будем добиваться того, чтобы управление киберпространством регулировалось такими правилами и нормами, которые будут способствовать укреплению коллективной безопасности, защите демократических идеалов и глобальному экономическому росту, а также позволят противодействовать распространению цифрового авторитаризма. Соединенное Королевство будет придерживаться в киберпространстве

[9] www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy.

принципа верховенства права и будет подавать пример ответственного поведения государства и вносить вклад в накопление передового международного опыта, поощрять соблюдение правил, противодействовать кибератакам, а также добиваться того, чтобы государства, допускающие безответственное поведение, были призваны к ответу. В тех случаях, когда это необходимо, мы будем формулировать правила таким образом, чтобы наступательные киберсредства разрабатывались и использовались ответственно и с соблюдением норм международного права.

Кроме того, мы намерены:

- бороться за обеспечение сохранности доступности и открытости в технологическом плане глобальной сети Интернет в интересах будущих поколений;
- обеспечивать защиту прав человека как в Интернете, так и за его пределами;
- прилагать усилия к тому, чтобы при разработке и внедрении новых технологий с самого начала учитывались принципы транспарентности и подотчетности;
- выступать за возможность передачи данных на территорию других государств, обеспечивая безопасный, надежный и открытый в технологическом плане трансграничный обмен данными с соблюдением стандартов защиты данных.

Одним из важнейших аспектов своего лидерства в области кибертехнологий Соединенное Королевство считает кибердипломатию, и созданная им сеть сотрудников, занятых в данной сфере, охватывает шесть континентов. В дополнение к осуществляемым нами программам по укреплению потенциала в области кибербезопасности мы инициировали межправительственные диалоги с 20 странами. В рамках этих диалогов мы продолжим развивать отношения с партнерами, с тем чтобы более убедительно демонстрировать необходимость формирования свободного, открытого, мирного и безопасного киберпространства, а также реагировать на злонамеренную деятельность в киберпространстве, осуществляемую по указанию государств, и сдерживать такую деятельность.

Мы продолжаем участвовать в работе целого ряда глобальных и региональных структур, посвященной обсуждению вопросов кибербезопасности, включая Рабочую группу открытого состава Организации Объединенных Наций и Группу правительственных экспертов Организации Объединенных Наций, Организацию по безопасности и сотрудничеству в Европе (ОБСЕ), Международный союз электросвязи и Глобальный форум по обмену опытом в области компьютерных технологий.

Соединенное Королевство считает себя в праве возлагать на государства ответственность за совершение злонамеренных действий в киберпространстве и делает это, если считает, что это отвечает его интересам, а также во исполнение своего обязательства по обеспечению ясности и стабильности в киберпространстве. Мы по-прежнему считаем, что принятие решения об обвинении какого-либо государства в совершении злонамеренных действий в киберпространстве и, что крайне важно, обнародование такого решения, в конечном счете является политической прерогативой государств. С заявлениями на эту тему и другой соответствующей информацией можно ознакомиться на веб-сайтах www.gov.uk и www.ncsc.gov.uk.

В 2020 году Великобритания создала Национальные кибернетические войска. Она принадлежит к числу стран, которые публично подтвердили, что занимаются созданием такого потенциала. Национальные кибернетические войска проводят ответственные целевые наступательные кибероперации в поддержку приоритетов Соединенного Королевства в области национальной безопасности и сочетают в себе возможности сил обороны и разведки. Кибероперации, осуществляемые наряду с использованием дипломатических, экономических, политических и военных возможностей, могут включать:

- создание помех для работы мобильного телефона с целью лишить террориста возможности связаться с лицами из его списка контактов;
- содействие предотвращению использования киберпространства в качестве глобальной платформы для совершения серьезных преступлений, включая мошенничество и сексуальные надругательства над детьми;
- обеспечение защиты военных самолетов Соединенного Королевства от прицельного огня путем создания помех для систем целеуказания.

Соединенное Королевство стремится использовать свой киберпотенциал ответственно и с соблюдением законодательства Соединенного Королевства и норм международного права. Кибероперации осуществлялись и будут осуществляться в рамках действующих законов, включая Закон о разведывательных службах 1994 года и Закон о следственных полномочиях 2016 года. Благодаря этому кибероперации Соединенного Королевства проводятся ответственно, целенаправленно и соразмерно поставленным задачам.

Все государства-члены согласны друг с другом в том, что поощрение использования информационно-коммуникационных технологий (ИКТ) в мирных целях отвечает интересам всех государств. Великобритания подтверждает, что ИКТ сами по себе не являются «угрозой». Скорее, угроза или риск возникают тогда, когда государства (или другие субъекты) намеренно используют ИКТ в целях, несовместимых с международным миром и безопасностью, или когда их действия воспринимаются подобным образом. В этом контексте продолжение обсуждения вопроса о том, как государства понимают применение международного права в отношении деятельности в киберпространстве, является целесообразным шагом на пути к обеспечению транспарентности, предсказуемости и стабильности.

С наиболее актуальной информацией о подходах, применяемых Соединенным Королевством к вопросам кибербезопасности, и в том числе в отношении международного сотрудничества, можно ознакомиться на веб-сайтах www.gov.uk/government/cyber-security и www.ncsc.gov.uk.

Содержание концепций, упомянутых в докладах Группы правительственных экспертов

Соединенное Королевство с удовлетворением отмечает, что в ходе обоих процессов государства-члены одобрили мнения, изложенные в трех предыдущих консенсусных докладах Группы правительственных экспертов за 2010, 2013 и 2015 годы, в которых Группа констатировала, что нормы международного права применимы и к киберпространству, и установила для государств рамки ответственного поведения, которые представляют собой набор добровольных и необязывающих норм и мер по укреплению доверия, дополненный усилиями по наращиванию потенциала. Новые доклады, которые будут опубликованы в 2021 году, станут важным вкладом в расширение существующей нормативной базы.

Соединенное Королевство считает, что надлежащее применение всеми государствами рамок, представленных в существующих докладах, во всей их полноте, является подходящей отправной точкой для наших усилий по повышению стабильности в киберпространстве. Верным шагом вперед в этом отношении стали бы универсализация и введение в действие практики подготовки сводных оценок и рекомендаций. Исходя из этого, необходимо применение практических, прикладных подходов.

Существующие и новые угрозы

Что касается формирующихся тенденций, то во время пандемии коронавирусного заболевания (COVID-19) злоумышленники пользовались возникшим кризисом, избирая для нападений соответствующие цели, среди которых были больницы и другие объекты критически важной инфраструктуры, связанные со здравоохранением. Злоумышленники активно атаковали организации, участвующие как в национальных, так и в международных мероприятиях по борьбе с COVID-19. Среди этих организаций были органы здравоохранения, фармацевтические компании, научно-образовательные учреждения, организации, занимающиеся медицинскими исследованиями, и местные органы власти. Такие злоумышленники часто нападают на организации с целью сбора большого количества личной информации, хищения интеллектуальной собственности и разведывательных данных, представляющих интерес с точки зрения национальных приоритетов.

Одним из наиболее распространенных и разрушительных по своим последствиям типов инцидентов, урегулированием которых занимается Национальный центр по вопросам кибербезопасности Великобритании, является использование программ-вымогателей. В ежегодном обзоре за 2020 год[10] мы отмечали, что количество инцидентов, которыми пришлось заниматься Центру, превысило аналогичный показатель за предшествующий год более чем втрое. Кроме того, в Соединенном Королевстве наблюдался всплеск атак с использованием программ-вымогателей, от которых пострадал сектор образования — как раз в тот период, когда учебные заведения прилагали все усилия для организации обучения, приема и тестирования в режиме онлайн. Злоумышленники все чаще повышают ставки, угрожая публично раскрыть украденную информацию, если жертвы не захотят заплатить выкуп. Помимо этого, мы отмечаем, что злоумышленники используют все более изощренные методы, проводя в той или иной сети длительное время в поисках наиболее ценных для шифрования данных, а также любых хранящихся в Интернете резервных копий, препятствуя таким образом восстановлению данных.

Как международное право применяется в сфере использования информационно-коммуникационных технологий

Соединенное Королевство подтверждает, что соблюдение всех действующих принципов международного права, включая принцип уважения прав человека и основных свобод и принцип применения международного гуманитарного права к кибероперациям в условиях вооруженного конфликта, является частью нашей общей приверженности обеспечению ответственного поведения в киберпространстве. Международное право применяется здесь во всей своей полноте точно так же, как оно применяется к деятельности государства за пределами Интернета.

[10] www.ncsc.gov.uk/news/annual-review-2020.

В этой связи мы поддерживаем призыв Международного комитета Красного Креста ко всем государствам подтвердить, что нормы международного гуманитарного права применимы к проведению кибероперациий во время вооруженных конфликтов. Когда государства прибегают к проведению кибероперациий, эта деятельность регулируется нормами международного права, как и деятельность в любой другой сфере. Применение норм международного гуманитарного права к кибероперациям в условиях вооруженного конфликта позволяет обеспечить как защиту, так и ясность. Применение таких норм снижает аппетит сторон к продолжению конфликта и обеспечивает соблюдение существующего свода принципов и правил, направленных на сведение к минимуму гуманитарных последствий конфликта.

Вместе с тем мы считаем, что в индивидуальном порядке всем государствам следует пойти еще дальше и сформулировать свою собственную концепцию в отношении того, как нормы международного права могут применяться к киберпространству. Великобритания сделала это в 2018 году, когда Королевский адвокат и член парламента Джереми Райт, занимавший на тот момент должность Генерального прокурора, изложил позицию Соединенного Королевства относительно применения международного права к киберпространству. Именно тогда точка зрения Соединенного Королевства была впервые официально изложена одним из ее министров.

Кроме того, мы признаем необходимость укрепления потенциала в области международного права, что можно было бы обеспечить посредством организации практических учебных занятий по вопросам, связанным с нашим пониманием применения международного права. Укрепление потенциала в этой области может оказать ощутимое влияние на способность государств выработать собственную позицию и в будущем отстаивать национальные интересы в ходе переговоров, а также принимать меры, позволяющие избежать непреднамеренного увеличения цифрового разрыва.

Нормы, правила и принципы ответственного поведения государств

В сентябре 2019 года Соединенное Королевство представило Рабочей группе открытого состава документ, озаглавленный *Non-paper on efforts to implement norms of responsible State behaviour in cyberspace, as agreed in the United Nations Group of Governmental Expert reports of 2010, 2013 and 2015* («Неофициальный документ по вопросу об усилиях, прилагаемых для внедрения норм ответственного поведения государств в киберпространстве, согласованных в докладах Группы правительственных экспертов Организации Объединенных Наций от 2010, 2013 и 2015 годов»)[11]. Этот документ служит хорошим источником информации об усилиях Соединенного Королевства по внедрению норм ответственного поведения государств. Мы с удовлетворением отметили представленный Многосторонней консультативной группой по вопросам кибертехнологий Соединенного Королевства дополнительный документ[12], в котором содержатся предложения относительно того, как заинтересованные стороны могут поддержать государства в деле внедрения упомянутых норм.

По мнению Великобритании, для того чтобы нормы были эффективными, необходимо обеспечить их внедрение. Решающее значение в этом контексте имеют следующие факторы:

[11] https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/uk-un-norms-non-paper-oewg-submission-final.pdf.

[12] www.un.org/disarmament/wp-content/uploads/2019/12/efforts-implement-norms-uk-stakeholders-12419.pdf.

- информированность правительств и заинтересованных кругов, что позволит выработать общее понимание ценности этих норм и способствовать их принятию;
- наличие ресурсов, необходимых для внедрения этих норм. Внедрение данных норм может и должно стать элементом каждой национальной стратегии кибербезопасности. В 2019 году такая стратегия имелась лишь у 40 процентов государств. Соединенное Королевство продолжает оказывать поддержку ряду государств в формировании национального киберпотенциала;
- наличие методических указаний по внедрению передовых наработок в данной области. Соединенное Королевство считает, что доклад Группы правительственных экспертов станет подробным руководством по разработке первоначальных принципов ответственного поведения государств в киберпространстве, в чем заинтересованы многие государства. Подспорьем в накоплении передового опыта в этой области станут и упомянутые выше неофициальный документ и прилагающийся к нему дополнительный документ.

Меры по укреплению доверия

Соединенное Королевство считает, что государствам следует сосредоточиться не на разработке новых мер по укреплению доверия, а на актуализации уже существующих. Наряду с частным сектором, научными кругами и организациями гражданского общества, важную роль в деле универсализации и практического осуществления рекомендаций, вынесенных предыдущими группами правительственных экспертов, играют региональные организации. Несмотря на это, масштабы практической реализации мер по укреплению доверия по-прежнему невелики, что существенным образом снижает потенциальную эффективность нашей рамочной концепции.

Великобритания активно участвует в деятельности Неофициальной рабочей группы ОБСЕ по разработке мер по укреплению доверия в киберпространстве. Мы приняли разработанную ОБСЕ меру укрепления доверия 5, касающуюся наращивания потенциала, взяв на себя обязательство содействовать ее практической реализации государствами ОБСЕ. В 2019 году мы выступили организаторами обсуждения с участием 40 государств-членов, в ходе которого рассматривались возможные сценарии кибератак, с тем чтобы отработать на практике понимание и реализацию мер по укреплению доверия. В 2020 и 2021 годах Великобритания председательствовала в Комитете по вопросам безопасности ОБСЕ и воспользовалась этой ролью для проведения двух мероприятий, посвященных теме кибертехнологий.

Укрепление потенциала

Великобритания является одним из крупных двусторонних доноров в сфере укрепления киберпотенциала. Мы считаем, что Организация Объединенных Наций может воспользоваться своим организационным потенциалом, чтобы привлечь больше внимания к задаче по укреплению потенциала в области кибербезопасности и содействовать скоординированному применению передовых наработок. Для того чтобы эта деятельность была максимально эффективной и результативной, важно вовлечь в нее все заинтересованные стороны и избежать дублирования существующих инициатив. В сфере укрепления потенциала уже имеется такой эффективный координационный механизм, как Глобальный форум по обмену опытом в области компьютерных технологий. Кроме того, важным вкладом в достижение этой цели является наличие независимых

инструментов оценки потенциала и руководств по передовым методам работы, а также деятельность таких организаций, как Форум групп оперативного реагирования и обеспечения безопасности, созданный для взаимодействия различных групп реагирования на инциденты в области кибербезопасности.

В период 2019–2021 годов Великобритания была спонсором стипендиальной программы «Женщины в контексте международной безопасности и киберпространства». Мы особенно гордимся тем, что по линии этой программы способствовали увеличению числа женщин в составе Рабочей группы открытого состава.

Регулярный институциональный диалог

Соединенное Королевство является одним из авторов предложения, касающегося программы действий в поддержку проведения в рамках Организации Объединенных Наций инклюзивного регулярного институционального диалога по вопросам ответственного поведения государств в киберпространстве. Мы выступаем за продолжение усилий по доработке и утверждению этого предложения.

III. Ответы, полученные от межправительственных организаций

Европейский союз

[Подлинный текст на английском языке]
[31 мая 2021 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 глобальное, открытое, стабильное, мирное и безопасное киберпространство, основанное на верховенстве права, правах человека, основных свободах и демократических ценностях, которые обеспечивают социальное, экономическое и политическое развитие во всем мире.

По мере того как Интернет все больше становится частью нашей жизни, в киберпространстве возникает ряд тех же самых проблем, с которыми мы сталкиваемся в физическом мире. Киберпространство все чаще используется в политических и идеологических целях, а усиливающаяся поляризация на международном уровне препятствует эффективной реализации принципа многосторонности. Картину угроз еще больше осложняют геополитическая напряженность в вопросах глобального и открытого Интернета и контроля над технологиями в рамках всей цепочки поставок. Злонамеренные атаки на критически важную инфраструктуру представляют собой серьезный глобальный риск. Ограничения, налагаемые на доступ к Интернету и пользование им, активизация вредоносной деятельности в киберпространстве, в частности деятельности, затрагивающей безопасность и целостность продуктов и услуг, основанных на информационно-коммуникационных технологиях (ИКТ), угрожают глобальному и открытому киберпространству, а также верховенству права, основным правам, свободе и демократии. Европейский союз и его государства-члены регулярно выражали обеспокоенность по поводу таких вредоносных действий, которые подрывают основанный на правилах международный порядок и повышают риск возникновения конфликтов.

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

Европейский союз и его государства-члены решительно поддерживают вышеупомянутую концепцию открытого, свободного, 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 глобальную стабильность, продвигать 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 между государствами. Укрепление глобальной киберустойчивости является важнейшим элементом поддержания международного мира и стабильности, снижая риск возникновения конфликтов и способствуя решению проблем, связанных с цифровизацией экономики и общества. Глобальная киберустойчивость снижает способность потенциальных злоумышленников использовать информационно-коммуникационные технологии в неблаговидных целях и укрепляет способность государств эффективно реагировать на киберинциденты и преодолевать их последствия.

В стратегии кибербезопасности 2013 года под названием «Открытое, безопасное и защищенное киберпространство»[13], 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. Эти инструменты призваны укрепить ценности Европейского союза и способствовать формированию условий для роста цифровой экономики. Некоторые конкретные меры направлены на повышение кибербезопасности информационных систем, снижение киберпреступности и укрепление международной политики Европейского союза в области кибербезопасности и киберзащиты.

В феврале 2015 года в своих Заключениях по кибердипломатии[14] 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 применимость существующего международного права в киберпространстве и в области международной безопасности, актуальность норм поведения и

[13] 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».

[14] 6122/15. Заключения Совета относительно кибердипломатии.

важность управления Интернетом являются неотъемлемыми элементами общего и всеобъемлющего подхода Европейского союза к кибердипломатии.

Как явствует из результатов обзора Стратегии кибербезопасности 2013 года, 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 структур и с учетом уважения их компетенции и обязанностей. В 2017 году в совместном сообщении, озаглавленном «Устойчивость, сдерживание и оборона: обеспечение надежной кибербезопасности Европейского союза»[15] были определены масштаб задач и комплекс мер, предусмотренных на уровне Европейского союза и призванных лучше подготовить его к решению постоянно растущих проблем в сфере кибербезопасности.

Озабоченность в связи с этими проблемами послужила стимулом к разработке механизма совместного дипломатического реагирования Европейского союза на вредоносную деятельность в кибрепространстве — инструментария кибердипломатии[16]. Растущая способность и готовность государственных и негосударственных субъектов добиваться своих целей с помощью вредоносной деятельности в кибрепространстве должна вызывать у международного сообщества озабоченность. Такая деятельность может выливаться в международно-противоправные деяния и иметь дестабилизирующие и многоуровневые последствия, среди которых — повышенный риск 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 создания глобального, открытого, стабильного, мирного 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 кибербезопасной цифровой трансформации в условиях сложных угроз[17]. Стратегия кибербезопасности Европейского союза для цифрового десятилетия

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

[16] 10474/17. Заключения Совета относительно механизма совместного дипломатического реагирования Европейского союза на вредоносную деятельность в киберпространстве («Инструментарий кибердипломатии»).

[17] См. совместное сообщение для Европейского парламента и Совета, озаглавленное «Стратегия кибербезопасности Европейского союза для цифрового десятилетия», и документ 7290/21 (22 марта 2021 года) «Заключения Совета по стратегии кибербезопасности Европейского союза для цифрового десятилетия».

направлена на поощрение и защиту глобального, открытого, свободного, стабильного и безопасного киберпространства, основанного на правах человека, основных свободах, демократии и верховенстве права. Эта стратегия содержит конкретные предложения по обеспечению устойчивости к внешним воздействиям, 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 Европейскому союзу добиться соответствия нормам, правилам и принципам ответственного поведения государств, принятым Организацией Объединенных Наций.

Международная политика Европейского союза по вопросам киберпространства зиждется на уважении основных ценностей Европейского союза, определяет нормы ответственного поведения и призывает к применению существующих норм международного права в киберпространстве; она предусматривает оказание странам, не входящим в состав Европейского союза, помощи в наращивании потенциала в области кибербезопасности и направлена на стимулирование международного сотрудничества в регулировании и использовании киберпространства. Европейский союз продолжает работать с международными партнерами в целях расширения и поощрения глобального, открытого, стабильного и безопасного киберпространства, в котором уважается международное право, в частности Устав Организации Объединенных Наций, и соблюдаются добровольные, не имеющие обязательной силы нормы, правила и принципы ответственного поведения государств. Существует очевидная необходимость в продвижении свода норм Организации Объединенных Наций по ответственному поведению государств в киберпространстве как средства стимулирования эффективных многосторонних дебатов, направленных на укрепление мира и безопасности в киберпространстве. Совместно с 53 государствами — членами Организации Объединенных Наций Европейский союз предлагает разработать программу действий по поощрению ответственного поведения государств в киберпространстве. Такая программа действий, опирающаяся на существующий свод норм, одобренных Генеральной Ассамблеей, обеспечит постоянную платформу для сотрудничества и обмена передовым опытом в рамках Организации Объединенных Наций. Она позволит разрабатывать программы 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.

Содержание концепций, упомянутых в 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. При этом последние события в киберпространстве порождают постоянно меняющиеся вызовы.

Европейский союз и его государства-члены обеспокоены расширением масштабов вредоносной деятельности в кибрепространстве, включая злонамеренное использование информационно-коммуникационных технологий как государственными, так и негосударственными субъектами, а также увеличением 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, включая повышенный риск возникновения конфликта.

По мере продолжения пандемии коронавирусного заболевания (COVID-19) Европейский союз и его государства-члены регистрируют в киберпространстве все новые угрозы и вредоносные действия, направленные против основных операторов в государствах-членах и их международных партнеров, в том числе в секторе здравоохранения. Европейский союз и его государства-члены особенно обеспокоены участившимися в последнее время посягательствами на безопасность и неприкосновенность продуктов и услуг ИКТ, которые могут иметь системные последствия.

Европейский союз и его государства-члены осуждают эту вредоносную деятельность в киберпространстве и подчеркивают свою неизменную поддержку усилий по укреплению глобальной киберустойчивости. Любые попытки помешать функционированию критически важной инфраструктуры неприемлемы и могут поставить под угрозу жизни людей. Злонамеренное использование ИКТ уменьшает полезность Интернета и соответствующих технологий для общества в целом и свидетельствует о готовности некоторых субъектов поставить на кон международную безопасность и стабильность. Все субъекты должны воздерживаться от безответственных и дестабилизирующих действий в киберпространстве.

Как это предусмотрено в международном праве и консенсусных докладах групп правительственных экспертов Организации Объединенных Наций за 2010, 2013 и 2015 годы, Европейский союз и его государства-члены призывают каждую страну проявлять должную осмотрительность и принимать надлежащие меры в отношении субъектов, осуществляющих подобную деятельность с ее территории. Европейский союз и его государства-члены вновь подчеркивают, что государства не должны сознательно допускать того, чтобы их территория использовалась для совершения международно-противоправных деяний с применением ИКТ, а также должны отвечать на соответствующие просьбы другого государства о сдерживании вредоносной кибердеятельности, исходящей с их территории.

Кроме того, как признается в предыдущих докладах Группы правительственных экспертов и Рабочей группы открытого состава, подход Европейского союза к борьбе с киберугрозами в контексте международной безопасности должен оставаться технологически нейтральным ввиду уникального характер, присущего информационно-коммуникационным технологиям. Это соответствует концепции применимости существующего международного права к новым областям, в том числе к использованию новых технологий, которая была признана Организацией Объединенных Наций.

Европейский союз и его государства-члены могут только поддерживать развитие и применение таких основанных на использовании ИКТ технологий, систем и услуг, которые обеспечивают полное соблюдение применимого международного права и норм, в частности Устава Организации Объединенных Наций, а также международного гуманитарного права и прав человека.

Как международное право применяется 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 кибербезопасности может опираться только на существующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международные нормы в области 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 от 2010, 2013 и 2015 годов, а также принципы, установленные в пунктах 28 a)-28 f) доклада 2015 года и в докладах Рабочей группы открытого состава.

Международное право, в том числе международное гуманитарное право, включая принципы предосторожности, гуманности, военной необходимости, соразмерности и проведения различия, 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 свою убежденность в том, что международное право не призвано служить источником конфликта и что его предназначение — устанавливать нормы, регулирующие военные операции в целях ограничения их последствий и, в частности, защиты гражданского населения.

Кроме того, права человека и основные свободы, закрепленные в соответствующих международных договорах, должны уважаться и соблюдаться как в Интернете, так и в физическом мире. Европейский союз и его государства-члены приветствуют тот факт, что значение этих принципов было подтверждено Советом по правам человека[18] и Генеральной Ассамблеей.

По этим причинам Европейский союз и его государства-члены на данном этапе не призывают к разработке новых международно-правовых инструментов по вопросам киберпространства и не видят в этом необходимости, поскольку надлежащая международная правовая база уже существует.

Европейский союз и его государства-члены вновь заявляют о том, что они поддерживают продолжение диалога и сотрудничества, направленных на достижение общего понимания в отношении применимости существующего международного права к использованию ИКТ государствами, а также поддерживают усилия по внесению юридической ясности в вопрос о порядке применения такого права, поскольку это 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

[18] A/HRC/RES/20/8.

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 70/237, а также принимать к сведению результаты деятельности Рабочей группы открытого состава и продолжать осуществление согласованных норм и мер по укреплению доверия, которые играют важную роль в предотвращении конфликтов.

При использовании ИКТ Европейский союз и его государства-члены будут руководствоваться существующим международным правом, а также придерживаться добровольных норм, правил и принципов ответственного поведения государств, в частности применительно к киберпространству, которые были сформулированы в докладах Группы правительственных экспертов от 2010, 2013 и 2015 годов. Мы считаем, что для практического продвижения вперед нужно добиваться расширения сотрудничества и повышения прозрачности применительно к обмену передовым опытом, в том числе по вопросам, касающимся порядка применения существующих норм, разработанных Группой правительственных экспертов, и что при этом следует действовать через соответствующие инициативы и структуры, такие как региональные организации и учреждения, что будет способствовать повышению осведомленности и эффективному осуществлению согласованных норм ответственного поведения государств.

Меры по укреплению доверия

Эффективные механизмы государственного сотрудничества и взаимодействия в киберпространстве представляют собой важнейший компонент деятельности по предотвращению конфликтов. Региональные форумы зарекомендовали себя в качестве подходящих платформ, предоставляющих субъектам 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 устойчивости 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. Устойчивость 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 области борьбы с инцидентами в киберпространстве, 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 признают, 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 киберпотенциала, в частности по линии потенциального вспомогательного механизма, который будет работать под эгидой Организации Объединенных Наций и в рамках которого будут разрабатываться программы наращивания потенциала, учитывающие потребности, озвученные государствами-бенефициарами, например такого, как упомянутая выше программа действий.