Организация Объединенных Наций A/75/123

Генеральная Ассамблея

Distr.: General
23 June 2020
Russian
Original: Arabic/English/French/
Spanish

Семьдесят пятая сессия
Пункт 98 предварительного перечня*

Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности

Доклад Генерального секретаря

Содержание

* A/75/50.

I. Введение

1. 12 декабря 2019 года Генеральная Ассамблея приняла резолюцию 74/28, озаглавленную «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности» по пункту 93 повестки дня «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности».

2. В пункте 2 резолюции 74/28 Генеральная Ассамблея просила все государства-члены продолжать, принимая во внимание оценки и рекомендации, содержащиеся в докладах Группы правительственных экспертов по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности, информировать Генерального секретаря о своей точке зрения и об оценках по следующим вопросам:

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

b) содержание концепций, упомянутых в докладах Группы правительственных экспертов.

3. Во исполнение этой просьбы 27 января 2020 года всем государствам-членам была направлена вербальная нота с предложением представить информацию по этому вопросу. Поскольку вызванный коронавирусной инфекцией (COVID-19) кризис все еще продолжается, в целях содействия представлению государствами-членами мнений по вышеизложенным вопросам первоначальный срок представления докладов, установленный на 15 мая 2020 года, был продлен до 31 мая 2020 года.

4. Ответы, полученные на момент составления настоящего доклада, содержатся в разделах II и III. Дополнительные ответы, полученные после 31 мая 2020 года, будут опубликованы на веб-сайте Управления по вопросам разоружения (http://www.un.org/disarmament/ict-security) на том языке, на котором они были представлены.

II. Ответы, полученные от правительств

Армения

[Подлинный текст на английском языке]
[13 мая 2020 года]

Армения придает большое значение открытому, свободному, стабильному и безопасному киберпространству, в основе которого лежит всестороннее соблюдение принципов и норм международного права и Устава Организации Объединенных Наций во всей их совокупности. Учитывая глобальный характер киберпространства, важно защищать права и свободы человека в Интернете, особенно право на свободу мнений и их свободное выражение, которое включает право искать, получать и распространять информацию. Тем временем проблемы, связанные с использованием информационно-коммуникационных технологий (ИКТ) и киберпространством, имеют широкомасштабный и разнообразный характер. Поэтому международное сообщество должно объединить свои усилия в целях предотвращения неправомерного использования ИКТ и содействия их мирному и совместному использованию. С учетом этого Армения активно участвует в работе международных платформ по вопросам

сотрудничества, с тем чтобы повысить транспарентность, предсказуемость и стабильность в киберпространстве и снизить риски и угрозы, связанные с использованием ИКТ.

Армения в полной мере привержена тщательному осуществлению Конвенции Совета Европы о киберпреступности и Дополнительного протокола к ней, касающегося уголовной ответственности за акты расистского и ксенофобского характера, совершаемые через компьютерные системы. С 2019 года Армения активно участвует в реализации совместного проекта Европейского союза и Совета Европы “CyberEast”, направленного на укрепление потенциала в областях кибербезопасности, уголовного правосудия и сбора электронных доказательств. Кроме того, Армения добросовестно осуществляет меры по укреплению доверия Организации по безопасности и сотрудничеству в Европе (ОБСЕ) (решение Постоянного совета 1202) в целях снижения угроз, связанных с использованием ИКТ. В июле 2019 года Армения принимала группу экспертов из Отдела ОБСЕ по транснациональным угрозам, которая прибыла для проведения оценки ее национального потенциала в области расследования киберпреступлений и судебного преследования за их совершение. В ноябре 2019 года Отдел ОБСЕ по транснациональным угрозам организовал в Ереване совместную встречу за круглым столом, с тем чтобы обсудить с армянскими заинтересованными сторонами результаты вышеупомянутой оценки. Опираясь на оценочный доклад экспертов и выводы встречи за круглым столом, Отдел ОБСЕ по транснациональным угрозам подготовил концептуальную записку по данному вопросу, которая в будущем может послужить основанием для разработки проекта.

Содержание и выводы докладов, подготовленных Группой правительственных экспертов Организации Объединенных Наций в 2013–2015 годах, отражают позиции ограниченного числа государств — членов Организации Объединенных Наций, вовлеченных в процесс подготовки докладов Группы правительственных экспертов, что не способствовало выработке универсального и всеобъемлющего комплекса норм, приемлемых для всех государств-членов. В этой связи мы считаем, что Рабочая группа открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, функционирующая как всеохватная и транспарентная платформа для обсуждений между государствами-членами, может разработать всеобъемлющий и сводный перечень правил, норм и принципов, касающихся ответственного поведения государств по вопросам использования ИКТ и приемлемых для всех государств-членов.

Австралия

[Подлинный текст на английском языке]
[29 мая 2020 года]

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

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)

подтверждается, что существующие нормы международного права, в частности Устав Организации Объединенных Наций, применимы и необходимы для поддержания мира и стабильности и содействия созданию открытой, безопасной, стабильной, доступной и мирной информационно-коммуникационной среды. В докладах также сформулированы добровольные необязательные нормы ответственного поведения государства и признается необходимость принимать меры по укреплению доверия и скоординированным образом наращивать потенциал. В целом эти меры (международное право, нормы, меры укрепления доверия и наращивание потенциала) обеспечивают основу для безопасного, стабильного и процветающего киберпространства и часто упоминаются как рамки ответственного поведения государств.

Австралия подтверждает свое обязательство действовать в соответствии со сводными докладами Группы правительственных экспертов за 2010, 2013 и 2015 годы (A/65/201; A/68/98; A/70/174). Австралия принимает активное участие в работе шестой Группы правительственных экспертов и первой Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (учреждены согласно резолюции 73/266 и резолюции 73/27 соответственно).

Международное право

Позиция Австралии в отношении того, как международное право регулирует поведение государств в киберпространстве, изложена в Международной стратегии действий в области кибербезопасности (2017 год), к которой прилагается Дополнение по вопросам международного права 2019 года (оба документа размещены на веб-сайте Министерства иностранных дел и торговли https://www.dfat.gov.au/sites/default/files/application-of-international-law-to-cyberspace.pdf).

В феврале 2020 года Австралия опубликовала неофициальный документ под заголовком «Тематические исследования по применению международного права в киберпространстве» (размещен на веб-сайте Рабочей группы открытого состава https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/02/australian-international-law-case-studies-final-5-february-2020.pdf и веб-сайте Департамента иностранных дел и торговли https://www.dfat.gov.au/sites/default/files/australias-oewg-non-paper-case-studies-on-the-application-of-international-law-in-cyberspace.pdf).

Осуществление

Напомнив, что в 2015 году Генеральная Ассамблея призвала все государства — члены Организации Объединенных Наций «при использовании информационно-коммуникационных технологий руководствоваться докладом Группы правительственных экспертов 2015 года» (см. резолюцию 70/237), Австралия опубликовала обзорный доклад о том, как она соблюдает и реализует четыре ключевых компонента доклада Группы правительственных экспертов 2015 года: международное право, нормы ответственного поведения государства, меры по укреплению доверия и наращивание потенциала (размещен на веб-сайте Рабочей группы открытого состава https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf и веб-сайте Департамента иностранных дел и торговли Австралии https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/international-security-and-cyberspace).

В докладе Группы правительственных экспертов 2015 года освещены мероприятия по распространению передового опыта, которые осуществлялись или уже осуществляются во многих странах. Австралия призывает все страны провести обзор текущей деятельности, осуществляемой в соответствии с вышеуказанным докладом (применение международного права, осуществление норм ответственного поведения государств, меры по укреплению доверия и наращивание потенциала), а также выявить пробелы и (в случае необходимости) возможности, необходимые для устранения этих пробелов. Вместе с Мексикой и 24 другими странами Австралия с удовлетворением представила Рабочей группе открытого состава (учреждена в соответствии с резолюцией 73/27) предложение о проведении обзора национальных мер по осуществлению резолюции 70/237 Генеральной Ассамблеи (размещено на веб-сайте Рабочей группы открытого состава https://front.un-arm.org/wp-content/uploads/2020/04/final-joint-oewg-proposal-survey-of-national-implementation-16-april-2020.pdf и веб-сайте Департамента иностранных дел и торговли https://www.dfat.gov.au/sites/default/files/joint-oewg-proposal-survey-of-national-implementation-april-2020.pdf).

Гендерные вопросы

Как признается в повестке дня по вопросу о женщинах и мире и безопасности, женщины по-разному и по-особому испытывают воздействие конфликтов и угроз международному миру и безопасности. Австралия высоко оценивает недавний доклад Института Организации Объединенных Наций по исследованию проблем разоружения под заголовком «Сохраняющееся отставание», в котором рассматривается тема гендерного баланса в дипломатии по вопросам контроля над вооружениями, нераспространения и разоружения и в котором отмечается, что в Первом комитете наблюдается самая незначительная доля женщин-дипломатов среди всех главных комитетов Генеральной Ассамблеи. Стипендия «Женщины в контексте международной безопасности и киберпространства» — это совместная инициатива правительств Австралии, Соединенного Королевства, Канады, Нидерландов и Новой Зеландии. Она способствует более широкому участию женщин в дискуссиях Организации Объединенных Наций по вопросам международной безопасности, связанным с ответственным поведением государств в киберпространстве. Австралия будет и впредь предпринимать реальные шаги в поддержку активного и эффективного участия женщин в многосторонних обсуждениях, касающихся международной безопасности и разоружения.

Босния и Герцеговина

[Подлинный текст на английском языке]
[11 мая 2020 года]

Информация об усилиях, предпринимаемых на национальном уровне в Боснии и Герцеговине в целях укрепления информационной безопасности и содействия международному сотрудничеству в этой области

Настоящий доклад подготовлен на основе данных, полученных от следующих учреждений Боснии и Герцеговины: Министерство безопасности Боснии и Герцеговины, Министерство обороны Боснии и Герцеговины, Министерство транспорта и коммуникаций Боснии и Герцеговины, Федеральная полицейская администрация, Министерство внутренних дел Республики Сербской и Министерство научно-технического развития, высшего образования и информационного общества Республики Сербской. К числу учреждений, которые не предоставили данных Министерству безопасности Боснии и Герцеговины до момента

отправки доклада, относятся следующие: полиция округа Брчко и Федеральное министерство транспорта и коммуникаций.

Босния и Герцеговина подписала международные соглашения и конвенции, касающиеся информации и кибербезопасности. Наиболее известными из них являются Конвенция о киберпреступности и Соглашение о стабилизации и ассоциации. Конвенция была открыта для подписания 23 ноября 2001 года в Будапеште, а Президиум Боснии и Герцеговины принял решение о ратификации документа на своей 89-м заседании, состоявшемся 25 марта 2006 года. Таким образом, Босния и Герцеговина обязана принять законодательство и другие необходимые меры по борьбе с киберпреступностью, с тем чтобы согласовать их с учетом мнения других подписавших Конвенцию сторон относительно рассмотрения уголовных преступлений и сбора, обработки и хранения данных.

С точки зрения охваченных в Конвенции тем актуальное значение в Боснии и Герцеговине имеет следующее законодательство:

- уголовный кодекс Боснии и Герцеговины, «Официальный вестник Боснии и Герцеговины», № 3/03;
- уголовно-процессуальный кодекс, «Официальный вестник Боснии и Герцеговины», №№ 3/03, 32/03, 36/03, 26/04, 63/04, 13/05, 48/05, 46/06, 76/06, 29/07, 32/07, 53/07, 76/07, 15/08, 58/08, 12/09, 16/09, 93/09 и 72/13;
- уголовный кодекс Федерации Боснии и Герцеговины, «Официальный вестник Федерации Боснии и Герцеговины», №№ 36/03, 21/04, 69/04, 18/05, 42/10, 42/11, 59/14, 76/14, 46/16 и 75/17;
- уголовно-процессуальный кодекс Федерации Боснии и Герцеговины, «Официальный вестник Федерации Боснии и Герцеговины», №№ 35/03, 37/03, 56/03, 78/04, 28/05, 55/06, 27/07, 53/07, 09/09, 12/10, 08/13 и 59/14;
- уголовный кодекс Республики Сербской, «Официальный вестник Республики Сербской», №№ 64/17 и 104/18;
- уголовно-процессуальный кодекс Республики Сербской, «Официальный вестник Республики Сербской», №№ 53/12, 91/17 и 66/18;
- уголовный кодекс района Брчко, «Официальный вестник района Брчко», №№ 33/13, 26/16, 13/17 и 50/18;
- уголовно-процессуальный кодекс района Брчко, «Официальный вестник района Брчко», №№ 33/13, 27/14 и 3/19.

Государственный уровень

Руководствуясь вышеизложенным и осознавая риски, которые могут возникнуть в киберпространстве, Министерство безопасности Боснии и Герцеговины провело следующие мероприятия.

По предложению Министерства безопасности Боснии и Герцеговины Совет министров Боснии и Герцеговины на своем 93-м заседании, состоявшемся 8 марта 2017 года, принял решение о создании Группы реагирования на компьютерные инциденты для учреждений Боснии и Герцеговины, которое было опубликовано в «Официальном вестнике Боснии и Герцеговины» № 25/17; таким образом, была учреждена Группа реагирования на компьютерные инциденты, которая была передана в ведение Управления информационных технологий и телекоммуникационных систем Министерства безопасности Боснии и Герцеговины.

В соответствии со статьей 4 вышеупомянутого решения Министерству безопасности Боснии и Герцеговины необходимо изменить свою внутреннюю организацию и классификацию рабочих должностей, с тем чтобы обеспечить надлежащее функционирование Группы реагирования на компьютерные инциденты. Все необходимые и предусмотренные процедурой заключения, касающиеся изменения внутренней организации и структуризации учреждения, были получены в конце 2017 года и вместе со всеми подготовленными документами вызвали исключительно положительный отзыв.

Министерство безопасности Боснии и Герцеговины внесло необходимые изменения и корректировки в свою внутреннюю организацию и классификацию рабочих должностей, с тем чтобы обеспечить надлежащее функционирование Группы реагирования на компьютерные инциденты, и передало их на утверждение Совету министров Боснии и Герцеговины. В настоящее время ожидается, что Совет министров Боснии и Герцеговины даст свое согласие на предложенный свод правил. После получения согласия Министерство безопасности Боснии и Герцеговины приступит к оперативно-технической работе по созданию группы реагирования на компьютерные инциденты для учреждений Боснии и Герцеговины. Предлагаемое изменение внутренней организации предусматривает, что в новое подразделение Управления информационных технологий и телекоммуникационных систем будут дополнительно включены пять должностей.

Министерство безопасности Боснии и Герцеговины планирует укрепить Группу реагирования на компьютерные инциденты в оперативном, институциональном и техническом плане, стремясь к достижению стратегических целей этого органа (координация и сотрудничество с соответствующими органами в Боснии и Герцеговине, устранение и смягчение последствий инцидентов в области безопасности, вызванных несанкционированным доступом к информационно-коммуникационным системам в учреждениях Боснии и Герцеговины, повышение надежности таких систем в учреждениях Боснии и Герцеговины путем осуществления постоянной и самоотверженной работы, деятельность по предотвращению и минимизации возможностей возникновения инцидентов в области безопасности, оказание администраторам содействия в реагировании на инциденты в области безопасности и т.д.), осуществляя деятельность в соответствии со статьей 6 решения и формируя сеть групп реагирования на компьютерные инциденты в Боснии и Герцеговине.

Кроме того, по предложению Министерства безопасности Боснии и Герцеговины Совет министров Боснии и Герцеговины на своем 107-м заседании, состоявшемся 6 июля 2017 года, одобрил аналитический документ о согласовании законодательства в области кибербезопасности в Боснии и Герцеговине и обязал Министерство безопасности Боснии и Герцеговины активизировать деятельность по разработке стратегии обеспечения кибербезопасности в Боснии и Герцеговине.

В этой связи проводятся мероприятия по согласованию точек зрения на уровне структур и органов в отношении модели стратегического документа, который, с одной стороны, будет увязан с директивой Европейского союза по сетевой и информационной безопасности и, с другой стороны, будет соответствовать конституционному устройству Боснии и Герцеговины.

Под эгидой Организации по безопасности и сотрудничеству в Европе (ОБСЕ) была сформирована неофициальная рабочая группа. Эта группа, которая состоит из представителей компетентных/заинтересованных учреждений Боснии и Герцеговины, подготовила документ «Руководящие принципы разработки стратегических рамок обеспечения кибербезопасности в Боснии и Герцеговине».

Кроме того, Министерство безопасности Боснии и Герцеговины участвует в текущих мероприятиях по разработке новой стратегии предотвращения терроризма и борьбы с ним в Боснии и Герцеговине, которая должна охватывать вопрос использования цифровой среды для проведения этих мероприятий.

Министерство безопасности Боснии и Герцеговины активно участвует в работе Комитета по Конвенции Совета Европы о киберпреступности.

По предложению Министерства безопасности Боснии и Герцеговины Совет министров Боснии и Герцеговины на своем 80-м заседании, состоявшемся 10 ноября 2016 года, принял решение об учреждении межведомственной рабочей группы по осуществлению проекта, направленного на укрепление потенциала в области киберпреступности (“iPROCEEDS”) (опубликовано в «Официальном вестнике Боснии и Герцеговины», № 14/17).

В январе 2016 года Европейский союз и Совет Европы подписали соглашение об осуществлении регионального проекта “iPROCEEDS”, направленного на наращивание потенциала стран Юго-Восточной Европы в области борьбы с киберпреступностью и делающего упор на конфискации доходов от преступлений в Интернете или киберпреступлений. Продолжительность проекта составила 42 месяца. Проект финансировался по линии Европейского союза и Совета Европы, а его осуществлением занимается Управление по борьбе с киберпреступностью Совета Европы, расположенное в Бухаресте. Было предложено, чтобы проектная группа, представляющая Боснию и Герцеговину, состояла из представителей Министерства юстиции, обладающих компетентными знаниями о данных преступлениях, работников прокуратуры, полицейских, сотрудников Департамента финансовой разведки и других ведомств. Данная рабочая группа была сформирована с учетом вышеизложенных факторов.

Кроме того, Министерство безопасности Боснии и Герцеговины координирует работу членов группы по проекту “iPROCEEDS-2”, который с января 2020 года осуществляется в целях борьбы с преступными доходами в Интернете и обеспечения сохранности электронных улик в странах Юго-Восточной Европы и Турции. Работа по этому проекту будет опираться на результаты, достигнутые в ходе реализации проекта “iPROCEEDS” и будет направлена на оказание целевой поддержки в следующих областях проектной деятельности: a) законодательство, касающееся обеспечения сохранности электронных доказательств и доступа к данным при полном соблюдении основных прав и свобод, включая неприкосновенность частной жизни и защиту персональных данных; b) учет стандартов защиты персональной информации, установленных Европейским союзом и Советом Европы; c) содействие реализации политики и стратегий по вопросам киберпреступности и кибербезопасности; d) межведомственное и государственно-частное сотрудничество в деле расследования киберпреступлений и выявления доходов от преступлений в сети Интернет; e) системы информирования общественности о случаях мошенничества в сети Интернет и других киберпреступлениях; f) подготовка судей по таким вопросам, как киберпреступность, электронные доказательства, соответствующие финансовые расследования и меры по борьбе с отмыванием денег; и g) международное сотрудничество и обмен информацией в целях расследования киберпреступлений и выявления доходов от преступлений в сети Интернет. Продолжительность проекта составляет 42 месяца.

Министерство безопасности Боснии и Герцеговины успешно выполняет роль координатора в деле осуществления мер ОБСЕ по укреплению доверия. К числу мероприятий, которые были осуществлены за этот период, относятся, в частности, следующие: успешная работа по предоставлению отчетности и информированию об уровне кибербезопасности в Боснии и Герцеговине, участие

в деятельности межведомственной рабочей группы, сформированной на основании решения 1039 Постоянного совета, участие в семи мероприятиях по проверке связи, а также проведение в мае 2019 года субрегионального учебного мероприятия по вопросам кибербезопасности и безопасности в сфере ИКТ. Кроме того, мы оказали поддержку ОБСЕ, задействовав свои ресурсы и знания для организации нескольких местных конференций и семинаров.

Кроме того, Босния и Герцеговина была включена в региональный проект «Повышение квалификации работников системы уголовного правосудия, занимающихся вопросами борьбы с киберпреступностью в странах Юго-Восточной Европы». Этот проект финансируется правительствами Германии и Соединенных Штатов Америки и реализуется Департаментом транснациональных угроз ОБСЕ в сотрудничестве с представителями стран региона (Албания, Босния и Герцеговина, Черногория, Косово[1], Сербия и Северная Македония) и полевыми миссиями ОБСЕ. Основная цель проекта — обучение и подготовка экспертов, работающих по делам об организованной преступности в киберпространстве. Проект осуществлялся в период 2017–2019 годов и способствовал разработке всеобъемлющих общих стратегических рамок, предназначенных для решения вопросов и преодоления угроз в сфере кибербезопасности, укрепления существующего потенциала в области борьбы с киберпреступностью и реагирования на опасность подрыва кибербезопасности. Министерство безопасности Боснии и Герцеговины играло в этом проекте координирующую роль.

Министерство обороны Боснии и Герцеговины проводит мероприятия, с тем чтобы к 2023 году в пределах своей юрисдикции создать эффективную и устойчивую систему кибербезопасности. Если говорить о ситуации на сегодняшний день, то 4 октября 2017 года Министерство приняло Стратегию кибербезопасности для оборонного сектора. 27 декабря 2017 года был принят подробный план реализации этой стратегии. В сфере безопасности главным образом решаются следующие задачи: предотвращение инцидентов в сфере безопасности и реагирование на них; обучение и аттестация сотрудников, обеспечивающих кибербезопасность в оборонном секторе Боснии и Герцеговины; и повышение среди конечных пользователей осведомленности о безопасности информационно-коммуникационных систем. В целях решения вышеуказанных задач Министерство обороны Боснии и Герцеговины уже разработало или приняло ряд имплементационных документов.

Кроме того, Министерство обороны Боснии и Герцеговины начало процесс создания своей группы реагирования на компьютерные инциденты.

В рамках программы НАТО «Партнерства ради мира» Министерство обороны Боснии и Герцеговины обязано решать партнерскую задачу G7300 в сфере киберзащиты, которая предусматривает следующее: a) принятие стратегических, процедурных и прочих документов, с тем чтобы обеспечить реальный учет требований киберзащиты в ходе процедур и процессов оперативного планирования, соблюдение международных правил в киберпространстве, осуществление мер безопасности путем обмена информацией о рисках и оценку угроз для национальных и международных органов с точки зрения кибербезопасности; b) учреждение группы реагирования на компьютерные инциденты; c) формирование потенциала для обеспечения конфиденциальности, доступности и достоверности информации и информационных систем Министерства обороны Боснии и Герцеговины и вооруженных сил Боснии и Герцеговины; d) принятие программ по обучению и подготовке соответствующих специалистов и конечных пользователей; e) принятие образовательных программ путем организации

[1] Данное обозначение не влияет на позицию, занимаемую в отношении статуса.

национальных киберучений и семинаров, а также участие представителей Министерства обороны Боснии и Герцеговины и вооруженных сил Боснии и Герцеговины в международных киберучениях и семинарах.

По предложению Министерства транспорта и коммуникаций Боснии и Герцеговины и в сотрудничестве с Министерством безопасности Боснии и Герцеговины Совет министров Боснии и Герцеговины на своем 95-м заседании, состоявшемся 22 марта 2017 года, принял Стратегию управления информационной безопасностью для учреждений Боснии и Герцеговины на 2017–2022 годы.

В настоящее время Министерство транспорта и коммуникаций Боснии и Герцеговины совместно с Министерством безопасности Боснии и Герцеговины разрабатывает закон об информационной безопасности и защите сетевых и информационных систем с учетом директивы № 2016/1148 Европейского союза о безопасности сетевых и информационных систем. Кроме того, это министерство сотрудничало, в частности, с Глобальным центром по укреплению потенциала в области кибербезопасности Оксфордского университета, Всемирным банком и Глобальным центром развития в сфере кибербезопасности в целях подготовки доклада о диапазоне возможностей по оценке потенциала в сфере кибербезопасности в Боснии и Герцеговине.

Что касается будущей деятельности, то Министерство транспорта и коммуникаций Боснии и Герцеговины планирует предложить закон об электронной идентификации при оказании конфиденциальных услуг и заключении электронных сделок и разработать стратегию развития информационного общества в Боснии и Герцеговине.

Уровень субъектов

Федерация Боснии и Герцеговины

Признавая важность кибербезопасности, в 2015 году Федеральное полицейское управление создало подразделение по борьбе с киберпреступностью. Это подразделение, как и Центр судебно-медицинской экспертизы, имеет надлежащий персонал, знания и оборудование. В подразделении по борьбе с киберпреступностью работают 10 экспертов, а Центр судебно-медицинской экспертизы входит в Европейскую сеть судебно-экспертных учреждений. Кроме того, это учреждение совместно с ЮНИСЕФ, международной структурой «Эммаус» и организацией «Спасти детей» активно участвует в реализации проекта по предупреждению в Боснии и Герцеговине сексуальной эксплуатации детей и жестокого обращения с ними в цифровой среде. Кроме того, это учреждение внесло ощутимый вклад в реализацию вышеупомянутых проектов, таких как “iPROCEEDS” и «Повышение квалификации работников системы уголовного правосудия в области борьбы с киберпреступностью в странах Юго-Восточной Европы», а также играет важнейшую роль в реализации нового проекта “iPROCEEDS-2”.

В 2018 году Федерация Боснии и Герцеговины приняла решение об учреждении Рабочей группы по реагированию на компьютерные инциденты для учреждений Федерации Боснии и Герцеговины, которая имеет схожие с двумя вышеуказанными органами цели и задачи.

Республика Сербская

Министерство внутренних дел Республики Сербской сообщило о проведении ряда мероприятий в целях согласования законодательства этого субъекта с законодательством Европейского союза. В связи с этим оно утвердило директивные указания по вопросам развития на 2017–2021 годы и план действий по

реализации этих директивные указаний на 2017–2019 годы. Оно также приняло программу развития информационно-коммуникационных технологий на 2017–2021 годы, которая содержит цель по совершенствованию и интеграции информационно-коммуникационной системы. В соответствии с этим был обновлен закон о полиции и внутренних делах Республики Сербской, в результате чего были созданы механизмы соблюдения регламента № 910/2014 Европейского союза об электронной идентификации и доверительных услугах для заключения электронных транзакций на внутреннем рынке и директивы № 2016/1148 о безопасности сетевых и информационных систем.

По предложению Министерства внутренних дел Республики Сербской был принят закон о безопасности важнейшей инфраструктуры («Официальный вестник Республики Сербской», № 58/19), который заложил основу для реализации директивы № 2008/114/ЕС и директивы о безопасности сетевых и информационных систем. Таким образом, в целях реагирования на любой инцидент, в том числе в киберпространстве, этот субъект сформировал законодательный потенциал и определил важнейшие объекты инфраструктуры.

Кроме того, это учреждение участвовало в следующих проектах: проект 2015 года «Повышение качества и безопасности обмена информацией между правоохранительными органами Боснии и Герцеговины» (предусматривается Механизмом по оказанию помощи в период до присоединения), «Повышение квалификации работников системы уголовного правосудия в области борьбы с киберпреступностью», “iPROCEEDS” и “iPROCEEDS-2”. Данное министерство также подготавливает инфраструктуру для безопасного обмена данными с другими учреждениями и юридическими субъектами, а также предоставляет услуги с опорой на механизмы обеспечения безопасности, определенные в директивном регламенте Европейского союза об электронной идентификации и доверительных услугах для заключения электронных транзакций на внутреннем рынке. Кроме того, разрабатываются документы, связанные с примирением существующих механизмов в сфере информационной безопасности.

Министерство внутренних дел Республики Сербской также имеет специальное подразделение по борьбе с преступностью в сфере высоких технологий, а также, как и все другие правоохранительные органы Боснии и Герцеговины, сотрудничает со следующими структурами: Международная организация уголовной полиции, Агентство Европейского союза по сотрудничеству правоохранительных органов, Агентство Европейского союза по сотрудничеству в области уголовного правосудия, Управление по наркотикам и преступности, ОБСЕ, Европейский полицейский колледж, посольство Соединенных Штатов, Международная программа содействия профессиональной подготовке в области уголовных расследований, Международная полицейская ассоциация, Детский фонд Организации Объединенных Наций и многие другие посольства и международные организации. Сотрудничество охватывает такие сферы, как образование, подготовка кадров и обмен знаниями и данными.

Что касается дополнительных органов по обеспечению кибербезопасности в Боснии и Герцеговине, то в 2011 году Республика Сербская в качестве субъекта приняла закон об информационной безопасности («Официальный вестник Республики Сербской», № 70/11), в котором определены основные правила информационной безопасности. В соответствии с этим законом в бывшем Агентстве по вопросам информационного общества Республики Сербской (ныне — Министерство научно-технического развития, высшего образования и информационного общества) был сформирован такой орган информационной безопасности, как Группа реагирования на компьютерные инциденты. На этот орган возложена задача координировать деятельность по профилактике, защите от компьютерных

инцидентов и охране киберинфраструктуры как государственных органов, так и юридических и физических лиц. За последние два года этот орган создал Оперативный центр безопасности при правительстве Республики Сербской в целях обеспечения информационной безопасности соответствующей инфраструктуры. Кроме того, были проведены мероприятия по подготовке операторов и началась работа в три смены. Этот орган активно стремится получить аккредитацию или стать членом соответствующих международных организаций.

Канада

[Подлинный текст на английском/французском языках]
[7 мая 2020 года]

В сфере обеспечения кибербезопасности Канада:

- привержена делу укрепления международной стабильности и формирования свободного, открытого и безопасного киберпространства;
- считает, что международное право применимо к такой сфере, как использование государствами информационно-коммуникационных технологий, и укрепляет стабильность в киберпространстве;
- призывает государства соблюдать согласованные нормы поведения государств в киберпространстве, включая нормы, которые были изложены в одобренном Генеральной Ассамблеей докладе Группы правительственных экспертов по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности от 2015 года;
- считает, что практические меры по укреплению доверия являются проверенным методом укрепления стабильности в киберпространстве.

На национальном уровне Канада проявляет активность по целому ряду направлений:

- в июне 2018 года правительство, действуя при руководящей роли Министерства общественной безопасности Канады, опубликовало Национальную стратегию кибербезопасности Канады. Эта стратегия направлена на укрепление партнерских связей, с тем чтобы обеспечить безопасность важнейших киберсистем, функционирующих в рамках и вне рамок федерального правительства, и защитить канадцев и канадские предприятия при подключении к сети Интернет. Ее цель также заключается в том, чтобы более эффективно выявлять постоянно возникающие киберугрозы и повышать способность реагировать на них. Эта стратегия составлена с учетом трех важнейших целей: a) безопасность и устойчивость канадских систем; b) инновационный и адаптивный характер экосистемы киберпространства; и c) лидерство, управление и сотрудничество. Канада реализует цели этой стратегии, опираясь на Национальный план действий в области кибербезопасности 2019 года, в котором изложены конкретные инициативы на пятилетний период;
- в рамках усилий по реализации Национальной стратегии кибербезопасности в Канаде был создан Канадский центр кибербезопасности, который объединил правительственные оперативные подразделения по кибербезопасности в одну ориентированную на интересы общественности организацию. Функционируя как национальная группа Канады по реагированию на компьютерные инциденты, вышеуказанный центр служит единым источником получения экспертных консультаций, рекомендаций, услуг и

поддержки для правительства, владельцев и операторов важнейшей инфраструктуры, частного сектора и канадской общественности;

- в 2018 году в Национальную стратегию кибербезопасности Канады было также включено положение о финансировании новой структуры —Национальной координационной группы по киберпреступности. Функционируя под управлением Королевской канадской конной полиции, эта группа будет обслуживать все канадские полицейские учреждения и будет сотрудничать с партнерами из государственного и частного секторов. Эта группа, которая будет функционировать на полную мощь к 2023 году, координирует и стимулирует работу по расследованию киберпреступлений в различных юрисдикциях Канады и на международном уровне;

- в 2018 году Королевская канадская конная полиция получила дополнительное финансирование для укрепления следственного и разведывательного оперативного потенциала и для расширения специальных технических знаний в поддержку мер по борьбе с киберпреступностью как внутри страны, так и на международном уровне.

На международном уровне Канада проявляет активность по целому ряду направлений:

- Канада взаимодействует с международным сообществом, государствами-единомышленниками и союзниками на многочисленных международных форумах в целях укрепления международной кибербезопасности. Например, Канада продолжает содействовать развитию международного права и соблюдению согласованных норм поведения государств в киберпространстве, включая нормы, утвержденные Генеральной Ассамблеей и изложенные в докладе Группы правительственных экспертов 2015 года. Канада также активно участвует в деятельности нынешней Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности и в соответствующих случаях выражает мнения по текущим обсуждениям в Группе правительственных экспертов. Канада надеется, что Рабочая группа открытого состава будет, в частности, способствовать соблюдению согласованных норм и учитывать гендерные аспекты кибербезопасности;

- на многосторонних форумах Организации Объединенных Наций Канада стремится к совершенствованию норм и стандартов и настоятельно призывает государства соблюдать свои обязательства в области прав человека. При этом предусматривается решение проблемы насилия в отношении женщин и девочек с использованием информационно-коммуникационных технологий и обеспечение их безопасности и личной неприкосновенности в реальной жизни и в сети Интернет. Канада стремится к достижению этих целей различными способами, в том числе путем руководства усилиями по подготовке резолюции Совета по правам человека о ликвидации насилия в отношении женщин и девочек в цифровом пространстве;

- руководствуясь своей оборонной стратегией 2017 года «Сила, безопасность, взаимодействие», Канада предпринимает усилия по сдерживанию злонамеренной деятельности в киберпространстве и реагированию на нее, в том числе путем использования своего кибернетического потенциала в поддержку военных операций. К имеющемуся кибернетическому потенциалу канадских вооруженных сил предъявляются такие же строгие требования, как и к другим видам военного потенциала, включая применимые национальные и международные законы и обязательства и правила применения вооруженной силы;

- на саммите в Шарлевуа, который состоялся в июне 2018 года, лидеры Группы семи объявили о создании Механизма быстрого реагирования. На этот механизм возложена задача координировать усилия, которые предпринимаются в рамках Группы семи с целью выявлять и реагировать на различные эволюционирующие угрозы для наших демократических государств, включая дезинформацию, путем обмена информацией, осуществления ее анализа и выявления возможностей для принятия скоординированных ответных мер. Данный механизм призван функционировать в интересах членов Группы семи и международного сообщества в целом, устраняя широкий спектр угроз для демократии.

К числу других предпринимаемых в настоящее время международных усилий относятся следующие:

- с 2015 года Канада обязуется выделить более 4 млн долл США на поддержку проектов по укреплению потенциала в области кибербезопасности. В рамках реализации программы стипендий «Женщины в киберпространстве», которая направлена на поощрение реального участия женщин в переговорах Организации Объединенных Наций по вопросам кибербезопасности, Канада также финансирует участие женщин-дипломатов из стран Северной и Южной Америки в деятельности Рабочей группы открытого состава;

- Канада поддерживает усилия Организации Североатлантического договора по укреплению киберзащиты Альянса и ряда союзников;

- Канада стремится осуществлять меры по укреплению доверия на различных форумах, включая форумы Организации по безопасности и сотрудничеству в Европе, форумы Организации американских государств (ОАГ) и Региональный форум Ассоциации государств Юго-Восточной Азии (АСЕАН);

- Канада является активным членом Коалиции за свободу в Интернете, которая представляет собой международную многостороннюю организацию по защите прав человека в Интернете и в рамках которой она возглавляет многостороннюю целевую группу по искусственному интеллекту и правам человека. Канада по-прежнему привержена продвижению глобальных усилий по обеспечению безопасности и стабильности в киберпространстве на благо всех людей.

Колумбия

[Подлинный текст на испанском языке]
[29 мая 2020 года]

В соответствии с резолюцией 74/28 Генеральной Ассамблеи, озаглавленной «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности», Колумбия, исходя из оценок и рекомендаций, содержащихся в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, хотела бы представить Генеральному секретарю свои мнения и замечания относительно следующих вопросов:

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

- содержание концепций, упомянутых в докладах Группы правительственных экспертов.

Введение

В широком смысле Колумбия выступает за свободную, открытую и безопасную цифровую среду, в которой гарантируется сетевой нейтралитет, и в этой связи считает важным продолжать уделять первоочередное внимание наращиванию потенциала и сотрудничеству на основе международного права и существующих норм и конвенций, а также осуществлению мер укрепления доверия в киберпространстве.

Что касается цифровой безопасности, то Колумбия прилагает значительные усилия в сфере кибертехнологий, стремясь к укреплению межведомственной координации на самом высоком уровне, с тем чтобы сделать киберпространство более безопасным.

В соответствии с принятой в 2016 году государственной политикой в области цифровой безопасности был создан Комитет цифровой безопасности, в работе которого принимают участие органы, занимающиеся данным вопросом, и который призван выполнять координирующую функцию в случае возможных кризисов в области национальной кибербезопасности. Руководство Комитетом осуществляет национальный координатор, которым в настоящее время является Советник Президента по экономическим вопросам и цифровой трансформации. Функции технического секретариата Комитета выполняет Министерство информационных технологий и связи.

Перечисленные ниже структуры созданы в целях координации деятельности по анализу и обновлению политики и нормативно-правовых рамок, регулирующих вопросы цифровой безопасности, и по пересмотру международной повестки дня, а также в целях обеспечения национальной обороны и безопасности в цифровой среде, с тем чтобы направить усилия на смягчение последствий кибератак и противодействие им, защиту критической национальной инфраструктуры и укрепление человеческого, технического, технологического и физического потенциала.

- **Группа реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий.** Орган Министерства обороны, задачей которого является координация действий, необходимых для защиты критической инфраструктуры Колумбии от чрезвычайных ситуаций в области кибербезопасности, ставящих под угрозу или подрывающих национальную безопасность и оборону. Этот орган отвечает за реагирование на компьютерные инциденты.

- **Объединенное кибернетическое командование вооруженных сил.** Руководящий орган, занимающийся управлением совместными кибероперациями, а также их планированием, координацией, интеграцией, проведением и синхронизацией. Его задачи заключаются в принятии мер киберзащиты и проведении военных кибероперациий на стратегическом уровне для обеспечения национальной безопасности и обороны в киберпространстве, включая координацию деятельности, связанной с объектами критической инфраструктуры.

- **Центр развития потенциала Колумбии в области кибербезопасности при Полицейском кибернетическом центре.** Эта структура является подразделением Управления Национальной полиции по расследованию уголовных преступлений и сотрудничеству с Интерполом и отвечает за разработку стратегий, программ и проектов в области цифровой безопасности,

кибербезопасности и проведения уголовных расследований для защиты распространяемой в киберпространстве информации и данных лиц, проживающих на территории страны.

- **Группа реагирования на инциденты в области компьютерной безопасности.** В Колумбии функционируют группы реагирования, относящиеся к правительственным и финансовым структурам, а также секторальные и частные группы реагирования. На региональном уровне Колумбия, являясь членом Организации американских государств (ОАГ), входит в сеть, объединяющую группы реагирования на инциденты в области компьютерной безопасности стран Северной и Южной Америки и созданную в целях более эффективного распространения соответствующих оповещений в данном регионе.

Колумбия согласна с необходимостью укреплять координацию и сотрудничество между государствами для изучения существующих угроз и возможных совместных мер противодействия им. В частности, большое значение имеет укрепление международного сотрудничества, понимаемого не только как передача знаний, технологий и передового опыта, но и как совместные и скоординированные действия.

Менее развитым в технологическом отношении странам крайне важно заключать соглашения и договоры, предусматривающие недопустимость использования киберпространства как плацдарма для эскалации конфликта ввиду возможных последствий, с которыми эти страны могут столкнуться, став объектом враждебных кибероперации или будучи использованы другими государствами в качестве «промежуточного звена» в конфликте ввиду недостаточного потенциала для принятия превентивных мер.

В этих странах любой ущерб, нанесенный критической информационной инфраструктуре, может иметь огромные последствия не только по причине зависимости от информационных технологий и перехода к автоматизации промышленных процессов с использованием Интернет-технологий, но и из-за непонимания существующих рисков и угроз, а также из-за нехватки ресурсов, необходимых для укрепления цифровой безопасности компаний, отвечающих за эксплуатацию этой инфраструктуры.

С учетом вышесказанного отсутствие потенциала должно учитываться в качестве одного из факторов риска, и, соответственно, необходимо создать механизмы международного сотрудничества для анализа рисков и укрепления потенциала.

Кроме того, отсутствие структуры категоризации рисков и недостаток мер по предупреждению инцидентов и защите критически важных видов деятельности представляют угрозу для государств, менее развитых с точки зрения цифровой безопасности. Еще одним фактором риска является отсутствие рамочной основы управления цифровой безопасностью, в свою очередь, осложняющее взаимодействие на межведомственном и международном уровнях.

Урегулирование новых угроз или угроз, которые могут возникнуть в будущем в связи с невероятно стремительным развитием технологий, а также вопросов, касающихся ответственного поведения государств в киберпространстве и безопасности информационных и телекоммуникационным систем, должно осуществляться на основе транснационального подхода, что позволит эффективно бороться с угрозами. Необходимо объединить усилия в целях оперативного распространения информации, включая ответственный обмен информацией о факторах уязвимости, а также в целях эффективного реагирования на потенциальные угрозы.

Колумбия вновь заявляет о своей полной готовности продолжать работу по координации и укреплению сотрудничества в целях изучения существующих и потенциальных угроз, а также возможных мер, в том числе совместных, по борьбе с ними.

Добровольные нормы, правила и принципы ответственного поведения государств

Колумбия полностью согласна с концепциями, соображениями, толкованиями и рекомендациями, изложенными в докладах групп правительственных экспертов, и в частности в докладе действующей группы от 2015 года, подготовленном на основе работы ее предшественниц и содержавшем рекомендации, которые были одобрены в том же году Генеральной Ассамблеей в качестве руководства по использованию ИКТ государствами-членами.

В краткосрочной перспективе необходимо приложить усилия для широкого распространения и выполнения этих рекомендаций. Колумбия считает, что в настоящее время потребность в каком-либо юридически обязывающем документе в данной области отсутствует.

Для укрепления национального потенциала по осуществлению упомянутых выше положений большое значение имеет и международное сотрудничество.

В соответствии с целями Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, Колумбия вновь заявляет о своей готовности к сотрудничеству в деле разработки и принятия мер по повышению стабильности и безопасности использования ИКТ и предупреждению совершения в сфере ИКТ действий, признаваемых вредоносными или способных поставить под угрозу международный мир и безопасность.

В этой связи 23 сентября 2019 года Колумбия поддержала предложенную Соединенными Штатами декларацию об ответственном поведении государств в киберпространстве, в рамках которой ряд стран обязался повысить уровень ответственности и стабильности в киберпространстве, прилагая совместные усилия в целях более эффективного реагирования на подрывную, деструктивную и дестабилизирующую злонамеренную деятельность в киберпространстве и сдерживания такой деятельности. При этом подчеркивается, что в основе ответственного поведения государств в киберпространстве должно лежать уважение норм международного права, соблюдение не имеющих обязательной силы стандартов поведения государств в мирное время и осуществление практических мер укрепления доверия.

Кроме того, Колумбия поддерживает опубликованный 12 ноября 2018 года Парижский призыв к доверию и безопасности в киберпространстве — инициативу правительства Франции, направленную на разработку общих принципов повышения безопасности в киберпространстве и получившую поддержку целого ряда стран, частных предприятий и организаций гражданского общества.

Кроме того, Колумбия поддерживает Крайстчерчский призыв к ликвидации материалов в Интернете, пропагандирующих терроризм и насильственный экстремизм, — инициативу правительств Франции и Новой Зеландии, представленную в мае 2019 года.

На национальном уровне Колумбия проводит государственную политику, которая изложена в документах Национального совета по социально-экономической политике. В 2011 году она официально утвердила кибербезопасность и кибероборону в качестве основополагающих элементов обеспечения

национальной обороны. Для этих целей правительство страны опубликовало документ № 3701 Национального совета по социально-экономической политике, который был озаглавлен «Руководящие принципы политики в области кибербезопасности и кибероборонь» и общая цель которого заключалась в укреплении потенциала государства по противодействию угрозам для национальной информационной безопасности и обороны (кибербезопасности и кибероборонь) путем создания надлежащей среды и условий для обеспечения защиты в киберпространстве. Прогресс был достигнут в трех основных областях: a) создание учреждений, занимающихся вопросами кибертехнологий, и опубликование методологических указаний в целях расширения возможностей государств по противодействию угрозам в киберпространстве; b) создание механизмов профессиональной подготовки по вопросам информационной безопасности и расширение сферы соответствующих исследований; и c) укрепление законодательства в области кибербезопасности.

В 2016 году Национальный совет по социально-экономической политике опубликовал документ № 3854 «Национальная политика в области цифровой безопасности», в котором основное внимание было уделено четырем аспектам: a) укреплению институциональных рамок; b) наращиванию потенциала различных заинтересованных сторон по выявлению, урегулированию, обработке и смягчению рисков в области цифровой безопасности в рамках их социально-экономической деятельности в цифровой среде; c) укреплению совместной ответственности; и d) включению подхода, основанного на управлении рисками, в деятельность различных заинтересованных сторон в цифровой среде.

С 2019 года разрабатывается государственная политика обеспечения доверия и безопасности в цифровой среде, предусматривающая, в частности, оценку и обновление системы управления цифровой безопасностью в целях ее оптимизации. В рамках этой деятельности было предложено создать национальную систему урегулирования инцидентов в области кибертехнологий, призванную выполнять следующие задачи: a) координировать институциональные усилия по оперативному урегулированию инцидентов в области кибертехнологий; b) служить официальным источником статистических данных о зафиксированных в стране инцидентах в области кибертехнологий; c) стандартизировать механизм периодической отчетности об инцидентах и факторах уязвимости в области кибертехнологий, что позволит выявлять и оценивать их, а также доводить до сведения заинтересованных сторон; и d) служить источником информации для принятия решений национальным правительством. Планируется разработка технического аспекта этой национальной системы урегулирования инцидентов в области кибертехнологий, чтобы обеспечить государственным органам безопасности доступ к информации, поступающей в режиме реального времени.

В рамках стратегических преобразований, предусмотренных в руководящих принципах политики в области обороны и безопасности, предполагается укреплять международное сотрудничество в области безопасности, а также развивать инновации, науку и технологии в целях укрепления потенциала оборонного сектора.

В контексте кибербезопасности и кибероборонь следует упомянуть о дипломатических усилиях, которые прилагаются в соответствии с концепцией безопасности на основе сотрудничества и способствуют развитию международных связей в данном секторе благодаря членству в стратегических альянсах. Так, являясь одним из глобальных партнеров Организации Североатлантического договора, страна участвует в обмене знаниями, а также, в рамках Индивидуальной программы партнерства и сотрудничества, занимается укреплением потенциала

национальных вооруженных сил и координации их действий по борьбе с угрозами в киберпространстве и по его защите.

Кроме того, Колумбия, опираясь на передовой международный опыт и стандарты, разработала руководящие принципы организации и функционирования групп реагирования на инциденты в области компьютерной безопасности для частных, государственных и смешанных структур в целях обеспечения оперативного реагирования на инциденты в области кибербезопасности, затрагивающие национальные интересы, поощрения сотрудничества, взаимодействия и международной взаимопомощи в области цифровой безопасности, кибербезопасности и кибероборонны между членами групп реагирования в Северной и Южной Америке и Европе, а также в интересах обмена опытом и передовыми наработками.

В свою очередь, Объединенное кибернетическое командование участвует в работе Иберо-американского форума по вопросам кибероборонны в целях развития сотрудничества, обмена накопленным опытом, укрепления потенциала в области управления транснациональными рисками и угрозами в киберпространстве и участия в национальных и международных учениях.

Полицейский кибернетический центр при посредстве функционирующего в нем Центра развития потенциала Колумбии в области кибербезопасности занимается аналитической работой, направляет предупредительные оповещения и проводит мероприятия, связанные с урегулированием инцидентов в области кибербезопасности, а также с инициированием следственных действий в рамках борьбы с киберпреступностью.

В свою очередь, такая структура, как Комиссия по регулированию связи, ставит перед собой следующие цели: a) создание механизмов содействия сотрудничеству в области цифровой безопасности между поставщиками услуг связи и Группой реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий; b) централизация данных различных секторов об инцидентах в области информационной безопасности в рамках структуры, отвечающей за управление этой информацией; и c) предоставление Группе реагирования необходимой информации для принятия мер по урегулированию инцидентов и повышения осведомленности о них в интересах различных сторон.

С этой целью Комиссия по регулированию связи в 2018 году вынесла постановление № 5569, в соответствии с которым, в частности, поставщики телекоммуникационных сетей и услуг обязаны внедрить систему управления информационной безопасностью, скорректировав свои процессы в целях обеспечения целостности, конфиденциальности и доступности данных.

Важно отметить, что при разработке политики цифровой безопасности были учтены рекомендации Организации экономического сотрудничества и развития, изложенные в документе *Digital Security Risk Management for Economic and Social Prosperity* («Управление рисками в области цифровой безопасности в интересах экономического и социального процветания»).

В соответствии с этими рекомендациями управление рисками в области цифровой безопасности должно начинаться с определения экономических и социальных целей, достижению которых должны способствовать меры безопасности, а также с планирования конкретных видов деятельности, с тем чтобы на следующем этапе оценить уровень риска, с которым сопряжены эти виды деятельности, и выяснить, каковы все его возможные последствия для достижения поставленных социальных и экономических целей.

Затем, на этапе обработки рисков, предстоит определить, какие изменения необходимо внести в существующие стратегии для того, чтобы повысить вероятность успешного осуществления соответствующей деятельности и сохранить неизменными поставленные цели, для чего необходимо решить, следует ли принять или снизить этот риск, перенести его на другие субъекты или же исключить его. В случае принятия решения о снижении этого риска можно выбрать и применить меры безопасности или рассмотреть возможность применения новаторского подхода или разработки мер обеспечения готовности к инцидентам.

С учетом вышеизложенного Колумбия при возникновении инцидентов, связанных с ИКТ, принимает во внимание всю соответствующую информацию, в том числе более широкий контекст произошедшего события, проблемы присвоения ответственности в ИКТ-среде, а также характер и масштабы последствий.

Что касается описания инцидентов и обязательного сообщения о них в компетентные органы, то Комиссия по регулированию связи, выделяя в своем постановлении различные категории инцидентов в области информационной безопасности, учитывала также руководящие принципы и передовые методы работы, изложенные в серии стандартов 27000 Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК) (и в частности, категории, предложенные в стандарте ИСО 27035-1). В соответствии с упомянутым выше постановлением при возникновении инцидентов в области информационной безопасности поставщики коммуникационных сетей и услуг после локализации инцидентов, ликвидации последствий и проведения восстановительных мероприятий должны направлять сообщения по электронной почте Группе реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий.

Что касается рекомендации, согласно которой «государства не должны заведомо позволять использовать их территорию для совершения международно-противоправных деяний с применением ИКТ», то, как уже говорилось выше, Колумбия через посредство Комитета цифровой безопасности, в состав которого входят, в частности, представители таких государственных органов по вопросам кибертехнологий, как Группа реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий, Объединенное кибернетическое командование, Полицейский кибернетический центр и правительственная группа реагирования на инциденты в области компьютерной безопасности, ведет работу по предотвращению любого рода киберинцидентов и реагированию на них на всей территории страны.

Колумбия стремится к сотрудничеству на международном уровне в деле обмена информацией, оказания взаимной помощи и уголовного преследования в связи с использованием ИКТ в террористических или иных преступных целях, а также осуществления других совместных мер противодействия таким угрозам.

В этой связи разрабатываемый в настоящее время новый документ Национального совета по социально-экономической политике, посвященный вопросам доверия и безопасности в цифровой среде, предусматривает создание и внедрение системы обмена информацией по вопросам кибертехнологий с целью повышения осведомленности заинтересованных сторон, взаимодействующих в цифровой среде на национальном и международном уровнях, о показателях, которыми измеряется их приверженность соответствующим целям. Эта система будет увязана с единым центральным журналом учета инцидентов в области цифровой безопасности.

Генеральная прокуратура Колумбии использует каналы международного сотрудничества в соответствии с действующими двусторонними и многосторонними соглашениями. Несмотря на это, представляется необходимым создать безопасный технологический канал связи или веб-сервис для прямых запросов и получения информации от поставщиков Интернет-услуг — в большинстве своем представителей частного сектора, — что позволит направлять и получать просьбы, обмениваться информацией и анализировать ее, с тем чтобы свести к минимуму время, требуемое для ответов на запросы о взаимной правовой помощи.

Недостатком существующих механизмов является длительное время реагирования, что является препятствием для осуществления уголовно-процессуальных действий. Иными словами, в момент получения ответа расследование находится на таком этапе, когда использовать эти данные в рамках уголовного процесса не представляется возможным.

Национальное разведывательное управление активно координирует свои действия с учреждениями-партнерами в некоторых странах в целях налаживания процедур обмена надлежащими оперативными данными, а также направления запросов о предоставлении более подробной информации по конкретным делам, требующим проведения дополнительного расследования или подтверждения установленных фактов.

Такая координация действий позволяет получить дополнительную информацию о выявленных в киберпространстве случаях или тенденциях, которые требуют сопоставления событий или предшествовавших им шагов для отслеживания деятельности злоумышленников в киберпространстве.

В соответствии с одной из рекомендаций государствам в целях обеспечения безопасного использования ИКТ следует соблюдать положения резолюций 20/8 и 26/13 Совета по правам человека о поощрении, защите и осуществлении прав человека в Интернете, а также резолюций 68/167 и 69/166 Генеральной Ассамблеи о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы гарантировать всестороннее уважение прав человека, включая право свободно выражать свое мнение. В связи с данной рекомендацией Конституционный суд Колумбии вынес ряд решений.

В частности, в унификационном постановлении № SU-420 от 2019 года указывается, что в Колумбии принцип свободного выражения мнений применяется в Интернете так же, как и в других средствах массовой информации, в связи с чем социальные сети не могут служить местом для диффамации; что, хотя в этом случае для публикации информации невозможно требовать наличия разрешения или предварительного согласования, тот факт, что свободному выражению мнений отдается определенный приоритет, не означает, что этот принцип соблюдается без каких-либо ограничений, и, соответственно, осуществление этого права любым лицом создает для него последствия, поскольку при этом затрагиваются интересы третьих лиц.

В 2017 году Комиссия по регулированию связи вынесла постановление № 5111 об установлении режима защиты прав потребителей коммуникационных услуг, внесении изменений в главу 1 раздела II постановления Комиссии № 5050 от 2016 года и утверждении других положений; в соответствии с этим режимом защиты прав потребителей поставщики телекоммуникационных сетей и услуг обязаны использовать соответствующие технические средства для предотвращения мошенничества в обслуживаемых ими сетях и периодически проверять эффективность этих механизмов. При этом, если пользователь направляет запрос, жалобу, претензию или требование о пересмотре решения в

связи с предполагаемым случаем мошенничества, то поставщик услуг должен выяснить причины случившегося.

Чтобы выяснить, какие изменения следует внести в законодательную и нормативно-правовую базу для укрепления цифровой безопасности и потенциала, в рамках разрабатываемой в настоящее время новой политики обеспечения доверия и безопасности в цифровой среде планируется провести диагностику, которая позволит определить, какие стандарты необходимо скорректировать в следующих областях: a) безопасность ИКТ; b) защита и отстаивание права на неприкосновенность частной жизни, свободу выражения мнений и других прав человека в Интернете; c) ответственное раскрытие информации о факторах уязвимости; d) защита данных; e) защита интересов потребителей; f) управление рисками и урегулирование инцидентов; g) деятельность центров реагирования на инциденты или других соответствующих структур; и h) создание секторальных групп реагирования на инциденты в области компьютерной безопасности. Эта диагностика будет проводиться с учетом интересов целого ряда сторон и позволит определить порядок корректировки действующей законодательной и нормативно-правовой базы.

Что касается рекомендаций относительно того, что государствам следует принимать надлежащие меры для защиты важнейших объектов инфраструктуры от угроз, связанных с ИКТ, то, помимо вышеизложенных мер, Колумбия, координируя свои действия с различными заинтересованными сторонами, прилагает усилия по разработке плана обеспечения безопасности и обороны важнейших объектов ИКТ-инфраструктуры, в котором будут изложены общие руководящие принципы для организаций, осуществляющих деятельность в соответствующем секторе. Создание этого документа станет первым шагом на пути к укреплению и объединению усилий по защите объектов инфраструктуры, признанных критически важными.

Что касается деятельности на международном уровне, то, как указывалось выше, Колумбия сотрудничает с другими государствами и реагирует на их просьбы об оказании помощи в деле смягчения последствий злонамеренных действий, связанных с ИКТ. Так, 16 марта 2020 года она присоединилась к Конвенции о киберпреступности. Кроме того, для того чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ, она предпринимает шаги по обеспечению надежности цепи поставки.

Что касается ответственного раскрытия информации о факторах уязвимости, связанных с ИКТ, и обмена соответствующей информацией об имеющихся ресурсах для устранения этих факторов в целях ограничения и возможной ликвидации потенциальных угроз для ИКТ или зависимой от них инфраструктуры, то в рамках разрабатываемой в настоящее время новой политики по обеспечению доверия и безопасности в цифровой среде планируется учредить процедуру ответственного раскрытия и распространения информации о факторах уязвимости в информационных системах и технологической инфраструктуре государственных учреждений, с тем чтобы соответствующая компетентная структура могла ликвидировать эти факторы уязвимости.

Что касается функционирования групп реагирования на чрезвычайные ситуации в области кибертехнологий или групп реагирования на инциденты в области компьютерной безопасности, то указания относительно создания таких групп были включены в документ № 3854 Национального совета по социально-экономической политике от 2016 года, в котором излагается национальная политика в области цифровой безопасности.

Добровольные меры укрепления доверия

Колумбия считает чрезвычайно важным продолжать разрабатывать и принимать меры укрепления доверия и безопасности в киберпространстве. На региональном уровне работа в этом направлении ведется по линии ОАГ.

В апреле 2017 года по инициативе Канады, Соединенных Штатов, Чили, Мексики и Колумбии была принята резолюция, в соответствии с которой в Межамериканском комитете по борьбе с терроризмом ОАГ была создана рабочая группа по сотрудничеству и мерам укрепления доверия в киберпространстве. В феврале 2018 года Колумбия была избрана председателем этой рабочей группы. На втором заседании группы, состоявшемся в апреле 2019 года в Чили, Колумбия передала свои полномочия Чили.

Меры укрепления доверия в области кибербезопасности, утвержденные ОАГ, заключаются в следующем:

1. Предоставлять информацию о национальной политике в области кибербезопасности, включая национальные стратегии, правительственные информационные документы, правовые рамки и другие документы, которые то или иное государство-член считает важными в этом контексте;

2. Уполномочить какую-либо из структур выполнять функции национального контактного центра на политическом уровне для обсуждения последствий киберугроз в Западном полушарии;

3. Наделить соответствующие подразделения в министерствах иностранных дел функциями контактных центров, в случае если таковые ранее отсутствовали, для поддержки усилий по налаживанию международного сотрудничества и взаимодействия в сфере кибербезопасности и киберпространства;

4. Развивать и укреплять деятельность по наращиванию потенциала, организуя такие мероприятия, как семинары, конференции и практикумы, посвященные вопросам кибердипломатии, для государственных должностных лиц и сотрудников частных предприятий;

5. Поощрять включение вопросов кибербезопасности и киберпространства в базовые учебные курсы, программу подготовки дипломатов и должностных лиц министерств иностранных дел и других государственных учреждений;

6. Содействовать сотрудничеству и обмену передовым опытом в области кибердипломатии, кибербезопасности и деятельности в киберпространстве путем создания рабочих групп, других механизмов диалога и подписания соглашений между государствами.

Следует отметить, что меры укрепления доверия, связанные с вопросами кибердипломатии, могут стать особенно важным вкладом в деятельность страны по линии ОАГ.

Кибердипломатия позволяет находить пути решения проблем, связанных с киберпространством. Для этого требуется не только активизировать участие государств в международных дискуссиях по вопросам кибербезопасности, что предполагает проведение подготовки дипломатических работников по этим вопросам, но также и обеспечивать активное участие экспертов в работе многосторонних форумов.

Помимо этого, представляется целесообразным проводить регулярные институциональные диалоги с широким кругом участников, а также расширять и поддерживать практику сотрудничества между группами реагирования на

чрезвычайные ситуации в компьютерной сфере и группами реагирования на инциденты в области компьютерной безопасности.

Что касается предложения о составлении всеобъемлющего перечня контактных центров, то из практических соображений предлагается создать их на различных уровнях, например, один контактный центр на политическом/дипломатическом уровне и несколько центров, выполняющих технические функции (на уровне полиции, прокуратуры, групп реагирования на чрезвычайные ситуации в компьютерной сфере и т.д.).

Важно будет определить субъекты, ответственные за управление информацией, и обеспечить ее обязательное регулярное обновление. Следует рассмотреть вопрос о разработке четкого и открытого протокола управления информацией, включая базы данных.

Что касается создания национальных контактных центров на техническом и политическом уровнях для урегулирования серьезных инцидентов, связанных с ИКТ, то в целях дальнейшей проработки различных аспектов цифровой безопасности в Министерстве информационных технологий и связи обеспечено четкое распределение ответственности за каждый из этих аспектов. Соответствующие данные могут быть предоставлены тем структурам, которым они будут необходимы.

Кроме того, Министерство информационных технологий и связи располагает базой контактных данных главных специалистов по информационным технологиям и информационной безопасности в государственных учреждениях и других заинтересованных структурах; эти специалисты участвуют в обсуждении рекомендаций по обеспечению безопасности в цифровой среде, а также в скоординированной деятельности на каждом этапе урегулирования инцидентов правительственными секторальными группами реагирования на инциденты в области безопасности компьютерных систем.

Что касается создания и поддержки двусторонних, региональных, субрегиональных и многосторонних консультативных механизмов и процессов в целях укрепления доверия между государствами и снижения риска недопонимания, эскалации напряженности и возникновения конфликтов в связи с инцидентами в сфере ИКТ, то, как уже говорилось, Колумбия активно участвует в работе различных международных форумов.

В частности, она принимает участие в прениях, проводимых в Организации Объединенных Наций (в Нью-Йорке, Вене и Женеве), а также в работе механизмов и в мероприятиях регионального уровня, главным образом в рамках ОАГ.

В рамках Группы по реализации Цифровой повестки дня Тихоокеанского альянса при поддержке со стороны созданной ОАГ Сети групп реагирования на инциденты в области компьютерной безопасности стран Северной и Южной Америки Колумбия участвует в проекте по обмену информацией о киберугрозах между государствами — членами Тихоокеанского альянса. В этой связи с 23 января 2020 года начала функционировать технологическая платформа для обмена информацией между группами стран-членов по реагированию на инциденты в области кибертехнологий. За функционирование соответствующего национального узла этой платформы отвечает Группа реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий.

Что касается деятельности на двустороннем уровне, то Колумбия заключила меморандум о взаимопонимании с Чили по вопросам киберпространства, кибербезопасности, кибероборонь, киберпреступности и киберразведки,

который был подписан 21 марта 2019 года министрами иностранных дел этих стран. Со стороны Колумбии в выполнении этого меморандума участвуют следующие структуры: Президентский совет по экономическим вопросам и цифровой трансформации, Министерство информационных технологий и связи, Министерство национальной обороны, Центр развития потенциала Колумбии в области кибербезопасности при Полицейском кибернетическом центре, Национальное разведывательное управление, Прокуратура, Министерство юстиции и права и Министерство иностранных дел.

15 апреля 2020 года в виртуальном формате состоялся обмен опытом в области цифровой безопасности между правительственными экспертами из Колумбии и Перу. Участники поделились друг с другом информацией о национальной политике и стратегиях, а также создали канал связи для оказания в будущем взаимной поддержки в ходе урегулирования инцидентов в области безопасности, имеющих отношение к ИКТ.

Кроме того, Колумбия участвует в работе советов по инновациям в области кибербезопасности, созданных по инициативе ОАГ и компании «Сиско» и представляющих собой площадки для взаимодействия основных лидеров в государственном и частном секторах, гражданского общества и научных кругов в интересах стимулирования инноваций, повышения уровня гражданской сознательности населения и распространения передового опыта в области кибербезопасности в соответствующем регионе. Создание таких площадок является важной вехой в процессе реализации мер укрепления доверия в киберпространстве и может способствовать проведению более эффективной политики цифровой безопасности на национальном и международном уровнях.

Запросы на международном уровне, относящиеся к сфере кибертехнологий, как правило, направляются через Управление по координации деятельности по предупреждению преступности Министерства иностранных дел.

Что касается активизации сотрудничества, в частности путем создания координационных центров для обмена информацией о злонамеренном использовании ИКТ и оказания помощи в проведении расследований, то важно отметить усилия различных органов и подразделений правительства по разработке национального протокола урегулирования инцидентов, который позволит координировать действия на ранних этапах возникновения компьютерных инцидентов, представляющих потенциальную угрозу экономическому и общественному строю или безопасности страны. Применение этого протокола представляется крайне важным, так как в нем предусмотрены действия, необходимые для выявления инцидента, анализа конкретных фактов и существующей угрозы, а также определения способа ее локализации или модификации.

В рамках Генеральной прокуратуры функционируют три подразделения по вопросам киберпреступности; в соответствии с запросами об оказании взаимной правовой помощи они предоставляют экспертную поддержку и помощь в расследовании таких преступлений, в составе которых фигурирует злонамеренное использование ИКТ.

Этим занимаются следующие подразделения: a) Специализированная прокуратура по борьбе с организованной преступностью; b) Специализированная прокуратура по обеспечению общественной безопасности; и c) Оперативно-следственное управление. Помимо оказания помощи в проведении расследований, эти группы экспертов содействуют внедрению в рамках данной структуры новых тенденций и применению передовых наработок в области борьбы с киберпреступностью и сбора электронных доказательств.

Управление прокуратуры по международным делам, занимаясь расследованиями, имеющими отношение к киберпреступности, опирается на поддержку различных высококвалифицированных прокуроров, а также трех вышеуказанных подразделений Прокуратуры по борьбе с киберпреступлениями.

Следует отметить поддержку со стороны Министерства юстиции Соединенных Штатов Америки, которое проводит профессиональную подготовку по вопросам, связанным с просьбами об оказании взаимной правовой помощи. В Соединенных Штатах органы власти, желающие получить доступ к хранимым электронным сообщениям, обязаны придерживаться определенных критериев или стандартов доказывания. Это выражается в том, что органы, направляющие соответствующий запрос, должны представить четко изложенные в хронологическом порядке факты, свидетельствующие о наличии разумных оснований для того, чтобы считать данные электронные записи важными и существенными для проводимого расследования. Необходимо показать, что имеются не просто презюмируемые, а обоснованные и надежные факты, указывающие на совершение преступления, и что соответствующая учетная запись электронной почты или социальной сети содержит информацию о расследуемом преступлении.

Аналогичным образом Национальное разведывательное управление в соответствии с просьбами стран, напрямую обращающихся к нему в рамках международного сотрудничества, проводит аналитическую работу и расследования на основе двусторонней координации.

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

Укрепление потенциала в сфере технологий имеет для Колумбии основополагающее значение.

Управление рисками в области цифровой безопасности — это та область, в которой государства, частный сектор и научные круги могут работать сообща, и в этой связи следует уделить внимание механизмам сотрудничества и международной помощи, способствующим достижению этой цели.

Важно, чтобы к анализу проблем кибербезопасности были привлечены различные заинтересованные стороны. Их помощь как в выявлении, так и в принятии превентивных мер безопасности и реагировании на инциденты и чрезвычайные ситуации является весьма ценной.

Важно, чтобы государства начинали этот процесс с выявления на внутреннем уровне тех областей, в которых необходимо наращивать потенциал. Для этих целей они могут опираться на модели технологической зрелости, разработанные на международном уровне.

Взяв их за основу, следует разработать планы, предусматривающие укрепление действующих мощностей, административного, кадрового и научного потенциала, физической и технологической инфраструктуры и предназначенные для органов и структур, отвечающих за кибербезопасность, а также за деятельность основных секторов. Кроме того, в рамках этих усилий по укреплению потенциала важно регулярно обновлять перечень объектов критической информационной инфраструктуры страны и планы их защиты, а также механизмы их согласования.

Этот вопрос касается всех, поэтому принципиально необходимо работать над созданием материалов образовательного характера по вопросам цифровой безопасности, с тем чтобы включать их в программы для различных уровней образования и неформальных курсов обучения.

Что касается разработки процедур оказания взаимной помощи в контексте реагирования на инциденты и решения краткосрочных проблем в области сетевой безопасности, включая процедуры, позволяющие ускорить оказание помощи, то в Колумбии создана национальная модель реагирования на инциденты, в рамках которой предусмотрен протокол урегулирования инцидентов на всей территории страны, в соответствии с которым органы по вопросам кибертехнологий действуют сообразно своим полномочиям и функциям.

В частности, была создана правительственная группа реагирования на инциденты в области компьютерной безопасности, призванная содействовать укреплению цифровой экосистемы в государственных структурах путем предоставления им бесплатных услуг. Перечень этих услуг состоит из трех разделов: упреждающие меры, меры реагирования и услуги в области управления безопасностью. Эти услуги включают мониторинг доступности веб-сайтов, анализ факторов уязвимости, отслеживание событий в области безопасности, поддержку в урегулировании инцидентов и реагировании на них, а также повышение осведомленности о методах урегулирования инцидентов.

Правительственная группа реагирования на инциденты в области компьютерной безопасности координирует свою деятельность с другими государственными органами по вопросам кибертехнологий (Группой реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий, Единым кибернетическим командованием и Полицейским кибернетическим центром) в целях урегулирования инцидентов в государственных структурах и, через посредство Комитета цифровой безопасности, участвует в разработке стратегий решения проблем, затрагивающих цифровую безопасность частных лиц и государства.

Помимо этого, в интересах содействия трансграничному сотрудничеству для устранения важнейших факторов уязвимости инфраструктуры, которые выходят за рамки национальных границ, Прокуратура координирует с другими странами региона осуществление стратегий своевременного и оперативного обмена информацией в ходе внутреннего расследования таких случаев, в которых, возможно, имело место нападение на важнейшие объекты инфраструктуры или действия, угрожающие их безопасности.

В свою очередь, Министерство информационных технологий и связи через посредство правительственной группы реагирования на инциденты в области компьютерной безопасности координирует свою деятельность с Группой реагирования на чрезвычайные ситуации в Колумбии в области кибертехнологий и Полицейским кибернетическим центром в целях проверки информации, поступающей из различных международных источников, что позволяет более оперативно принимать меры по смягчению последствий и расследованию инцидентов, когда это необходимо.

Что касается разработки стратегий устойчивости в рамках инициатив по укреплению потенциала в целях обеспечения безопасности ИКТ, то в различные механизмы осуществления государственной политики, о которых говорится в документах №№ 3711 и 3854 Национального совета по социально-экономической политике от 2016 года, были включены руководящие принципы и рекомендации по укреплению потенциала. Помимо этого, принимаются и другие административно-правовые меры по укреплению потенциала реагирования,

разработанные, в частности, Министерством информационных технологий и связи и Министерством обороны.

Так, в этой связи между правительством Колумбии и ОАГ были заключены соглашения о сотрудничестве, в соответствии с которыми стороны объединят свои усилия по линии технического сотрудничества, чтобы содействовать обновлению руководящих принципов обеспечения цифровой безопасности и укреплению технического потенциала и навыков в интересах управления рисками в области кибербезопасности путем реализации инициатив в двух основных областях: a) разработка политики и распространение информации о ней; и b) наращивание потенциала.

Генеральная прокуратура, действуя через Управление по международным делам, следует руководящим принципам и рекомендациям, принятым различными многосторонними организациями в целях укрепления безопасности в киберпространстве, стремясь надлежащим образом расследовать киберпреступления и тем самым, насколько это возможно, смягчать последствия безнаказанности.

Национальное разведывательное управление, стремясь содействовать укреплению национального потенциала в области кибертехнологий, приняло решение создать в системе разведывательных органов группу реагирования на инциденты в области компьютерной безопасности в качестве механизма координации действий в связи с событиями и инцидентами в этом секторе, а также обеспечить распространение информации технического характера о событиях и инцидентах и проводить расследование инцидентов в области кибертехнологий.

Помимо этого, первоочередное внимание в Колумбии уделяется повышению осведомленности о безопасности ИКТ, а также учету деятельности по укреплению потенциала в национальных планах и бюджетах для уделения должного внимания безопасности при планировании процесса развития и помощи. В этой связи в дополнение к уже упомянутой государственной политике в области обеспечения цифровой безопасности были разработаны информационно-разъяснительные программы по вопросам безопасности ИКТ в целях просвещения и уведомления учреждений и граждан.

Министерство информационных технологий и связи взяло на себя задачу по разработке программы укрепления потенциала, и, заключив соответствующие соглашения о сотрудничестве, организовало проведение учебных курсов, выдачу дипломов и сертификатов о прохождении подготовки в области информационной безопасности и управления информационными технологиями, обеспечив охват 1134 должностных лиц государственных учреждений на национальном и местном уровнях.

Среди этих инициатив следует отметить программу «Поговорим о цифровом правительстве», в рамках которой более 250 должностных лиц, занимающихся вопросами информационных технологий, и сотрудников служб безопасности государственных структур приняли участие в дискуссионном форуме на тему «Формирование потенциала по управлению безопасностью и рисками в цифровой среде».

В городе Перейра для государственных должностных лиц была организована соревновательная кампания на тему кибертехнологий («киберчеллендж»), в которой приняли участие 40 лидеров в области ИКТ. Кроме того, была проведена соревновательная кампания на тему кибербезопасности, в ходе которой участники решали проблемы и урегулировали ситуации, которые могут возникать в сетевой среде. Это мероприятие было проведено под эгидой ОАГ при

поддержке многонациональной компании «Тренд микро», занимающейся вопросами кибербезопасности.

В ходе семинаров на тему «Укрепление цифровой безопасности — улучшение положения в регионе» более 1400 должностных лиц, в том числе руководители отделов информационных технологий и сотрудники служб безопасности государственных структур, приняли участие в 25 совещаниях, состоявшихся в 24 городах Колумбии.

Благодаря поддержке ОАГ удалось повысить эффективность профессиональной подготовки в регионе. В частности, при финансовой поддержке Королевства Нидерландов несколько раз был проведен курс «Гаагский процесс: международные операции по обеспечению безопасности и вопросы киберпространства». Этот курс был проведен в Колумбии в 2019 году и, помимо колумбийских должностных лиц, участие в нем приняли другие делегаты из стран Латинской Америки и Карибского бассейна, являющиеся экспертами в вопросах кибербезопасности. Учебная программа этого курса включает такие темы, как суверенитет, юрисдикция, принцип должной осмотрительности, применение силы, международное право прав человека, морское право и мирные соглашения, а также другие смежные темы, причем во всех случаях кибероперации рассматриваются с научно-теоретической точки зрения.

Что касается укрепления потенциала в области криминалистической техники или совместных мер по борьбе с использованием ИКТ в террористических или иных преступных целях, то правительство Колумбии выступило принимающей стороной регионального практикума для Латинской Америки по вопросам получения электронных доказательств от частных поставщиков услуг связи в рамках борьбы с терроризмом и организованной преступностью в ходе трансграничных расследований; этот практикум был организован ОАГ, Исполнительным директоратом Контртеррористического комитета Организации Объединенных Наций, Управлением Организации Объединенных Наций по наркотикам и преступности; Международной ассоциацией прокуроров; Национальным координационным механизмом по вопросам цифровой безопасности и Министерством информационных технологий и связи. Участие в практикуме приняли делегаты из 13 стран Латинской Америки (должностные лица органов судебной полиции и других государственных учреждений); в целях укрепления международного сотрудничества в борьбе с терроризмом и организованной преступностью они прошли подготовку, в частности, по вопросам сбора трансграничных электронных доказательств, обновления законодательства в Соединенных Штатах, Канаде и Европейском союзе, оформления экстренных запросов о раскрытии информации и просьб о взаимной правовой помощи.

В течение последних трех лет Генеральная прокуратура обеспечивает командирование сотрудников судебной полиции из подразделений по борьбе с компьютерными преступлениями и компьютерной криминалистике для участия в важных семинарах и учебных мероприятиях, организуемых ОАГ и Реестром Интернет-адресов для стран Латинской Америки и Карибского бассейна, а также для совместной работы с прокурорами, имеющими опыт расследования дел, связанных с использованием технологий (в качестве объекта или средства совершения преступления), и руководящими такими расследованиями.

Кроме того, при поддержке частных организаций и местных университетов были проведены различные учебные курсы по вопросам борьбы с киберпреступностью и совершенствования таких методов работы, как применение протоколов, а также навыков работы с аппаратным и программным обеспечением для анализа электронных доказательств в целях сопоставления дел и выявления закономерностей.

Национальное разведывательное управление, координируя свои действия с функционирующей в системе разведывательных органов группой реагирования на инциденты в области компьютерной безопасности, планирует сформировать потенциал для тестирования возможности несанкционированного доступа к системам и анализа факторов уязвимости, проведения криминалистической экспертизы и восстановления цифровой информации, анализа вредоносных программ и цифровых артефактов, анализа приложений, создания лаборатории для разработки программного обеспечения с открытым исходным кодом, а также изучения киберфеноменов.

Во исполнение рекомендации относительно выработки региональных подходов к укреплению потенциала с учетом конкретных культурных, географических, политических, экономических или социальных аспектов в целях содействия применению подхода, адаптированного к каждому конкретному случаю, Министерство информационных технологий и связи через посредство Группы по вопросам безопасности и конфиденциальности Управления по вопросам цифрового правительства занимается внедрением модели информационной безопасности и конфиденциальности, которая объединяет инструменты, позволяющие государственным структурам на национальном и местном уровнях бороться с киберугрозами, и способствует формированию культуры безопасности, позволяющей лучше ориентироваться в ситуации при возникновении киберугроз, затрагивающих организации на транснациональном уровне.

Кроме того, в органах по вопросам уголовной политики ведется разработка национального плана, который включает аспекты, связанные с различными криминальными явлениями.

Национальное разведывательное управление работает над укреплением потенциала Национального разведывательного сообщества в области безопасного обмена информацией. В этой связи на основе координации с Агентством по сотрудничеству при президенте Колумбии осуществляется проект по профессиональной подготовке и формированию потенциала в области защиты и внедрения передовых методов работы для стран Карибского бассейна.

Как отмечалось выше, в интересах укрепления потенциала в области безопасности ИКТ Колумбия участвует в инициативах по развитию двустороннего и многостороннего сотрудничества, направленных на улучшение условий для эффективного оказания взаимной помощи при реагировании на инциденты, связанные с ИКТ.

Помимо этого, Министерство информационных технологий и связи разрабатывает стратегии сотрудничества с предприятиями, оказывающими услуги в области безопасности, и органами по вопросам кибертехнологий на международном уровне в целях обмена разведывательными данными об угрозах на стратегическом, тактическом и оперативном уровнях.

Применение норм международного права в контексте использования информационно-коммуникационных технологий

Колумбия считает, что нормы международного права, и в частности Устав Организации Объединенных Наций, а также нормы международного права прав человека и международного гуманитарного права, применимы как к «виртуальному», так и к «физическому» миру.

Она согласна с содержащимся в предисловии к докладу Группы правительственных экспертов от 2015 года заявлением тогдашнего Генерального секретаря о том, что «обеспечение стабильности и безопасности в киберпространстве может быть достигнуто лишь по линии международного сотрудничества,

причем основой такого сотрудничества должны являться нормы международного права и принципы, провозглашенные в Уставе Организации Объединенных Наций».

Исходя из этого, Колумбия считает, что общие концепции международного права могут быть применимы в киберпространстве с определенными уточнениями, обусловленными осуществлением деятельности в виртуальной среде и особенностями этой деятельности.

Учет различных возможных толкований вопросов, связанных с международным правом в киберпространстве, не исключает возможности подготовки руководств или справочников по применению норм международного публичного права в киберпространстве.

В этой связи весьма полезной могла бы оказаться практика осуществления Конвенции о киберпреступности, в которой содержатся указания относительно того, как следует применять ее положения и согласовывать их с достижениями в сфере технологий. Данная практика считается успешной, и ее можно было бы взять за образец.

С учетом того, что Генеральная Ассамблея Организации Объединенных Наций с удовлетворением отметила и рекомендовала к внедрению свод закрепленных в докладах групп правительственных экспертов международных правил, норм и принципов ответственного поведения государств, ближайшими задачами для Колумбии должны стать дальнейшее совершенствование этого свода норм и его более активное применение. Колумбия считает, что в настоящее время потребность в каком-либо юридически обязывающем документе в данной области отсутствует.

Кроме того, следует подчеркнуть, что Колумбия выполняет взятые на себя обязательства и соблюдает установленные гарантии.

Концептуальная база

Необходимо продолжить обсуждать в рамках многосторонних форумов доработку концептуальной базы, признанную необходимой для содействия дальнейшему уточнению понятий, связанных с международным миром и безопасностью в контексте использования ИКТ в правовой, технической и политической сферах, с учетом особенностей применения и новизны этих понятий.

Эти дискуссии имеют основополагающее значение для адаптации международных стандартов к проблемам, возникающим в киберпространстве, и для достижения консенсуса в отношении того, как международное право применяется в этой виртуальной среде. В этой связи Колумбия разделяет выводы Группы правительственных экспертов, содержащиеся в ее докладе от 2015 года, и готова к проведению более подробных дискуссий с другими делегациями в рамках Организации Объединенных Наций.

Только так можно будет обеспечить надлежащее использование ИКТ, которые имеют основополагающее значение для решения проблем, стоящих в настоящее время перед международным сообществом, и предотвратить такое использование этих технологий, которое противоречило бы целям и задачам Устава Организации Объединенных Наций, включая соблюдение гарантий поддержания международного мира и безопасности.

Использование новых революционных технологий в сфере услуг ведет к возникновению новой формы отношений в информационном обществе, которая, будучи основана на безопасной обработке информации и особой защите

персональных данных, будет способствовать популяризации преимуществ технического прогресса и повышению его роли в социально-экономическом развитии.

Исходя из этого, представляется крайне важным укрепить руководящую роль правительств, с тем чтобы, руководствуясь международной практикой устранения рисков в области цифровой безопасности, выработать новую стратегическую концепцию, в которой будут учтены принципы ответственного поведения государств, всеохватного участия в международных дискуссионных форумах по вопросам цифровой безопасности, а также транспарентности и предсказуемости действий государств по отношению к партнерам, с тем чтобы уменьшить риск недопонимания, эскалации напряженности и возникновения конфликтов, связанных с цифровой безопасностью.

И наконец, осуществление стратегий и принятие мер в целях ответственного использования цифровой среды способствуют миростроительству благодаря созданию надлежащих условий для сосуществования в цифровом пространстве, основанного на уважении, поощрении свободного выражения мнений и корректного речевого поведения в сети Интернет, в интересах использования преимуществ ИКТ и более успешной адаптации к цифровому миру будущего.

Дания

[Подлинный текст на английском языке]
[29 мая 2020 года]

Как и остальной мир, Дания все активнее внедряет подключение к Интернету. Войдя в нашу повседневную жизнь, цифровые решения помогают стимулировать экономический рост. Для Дании, которая является одной из наиболее цифровизированных стран мира, жизненно важно содействовать формированию глобального, открытого, стабильного, мирного и безопасного киберпространства, в котором в полной мере соблюдались бы права человека, основные свободы и принцип верховенства права.

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности и развития международного сотрудничества 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, что на цели укрепления кибербезопасности и кибероборонны будет выделено 1,4 млрд датских крон и что тем самым будет усилена наша жизнестойкость. В Датской стратегии в области кибернетической и информационной безопасности на 2018–2021 годы предусматриваются дальнейшие меры по укреплению кибербезопасности. Посредством реализации 25 инициатив и шести целевых стратегий в секторах, которые до сих пор определяются как критически значимые (энергетика, финансы, транспорт, здравоохранение, телекоммуникации и морское судоходство), Дания усилила технологическую устойчивость своей цифровой инфраструктуры, повысила уровень знаний и навыков среди граждан, предпринимателей и представителей органов власти, а также укрепила координацию и сотрудничество в области кибербезопасности. При этом в датское законодательство были полностью перенесены положения Директивы Европейского союза по безопасности сетевых и информационных систем.

В рамках Датской 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 специализированных секторальных подразделений и был учрежден Центр кибербезопасности; особое внимание при этом уделяется обмену опытом по вопросам информационной и кибернетической безопасности. В работе форума также принимают участие Агентство по цифровизации и Служба безопасности и разведки Дании.

Чтобы иметь достаточно квалифицированный персонал для выявления и отражения направленных против Дании кибератак, в частности против ее критически важной инфраструктуры, Центр кибербезопасности также создал Академию киберзащиты, в которой проводится интенсивная подготовка. В 2019 году ее закончили 15 выпускников, которые сейчас работают в оперативном подразделении Центра. Помимо Академии Центр кибербезопасности также поддерживает образовательно-исследовательскую деятельность в области кибербезопасности. Например, в 2019 году Центр кибербезопасности совместно с Копенгагенской школой дизайна и технологий, Ольборгским университетом, Университетом Южной Дании, Копенгагенской школой бизнеса и Техническим университетом Дании организовал первые в истории летние курсы по кибербезопасности.

В 2019 году был учрежден государственно-частный Совет кибербезопасности (“Cybersikkerhedsråd”), с тем чтобы оценивать работу национальных органов власти и частного сектора, укреплять цифровую демократию и углублять знания об угрозах и возможностях в свете цифровизации и новых технологий.

Наряду с реализацией Датской стратегии в области кибернетической и информационной безопасности на 2018–2021 годы, Дания укрепляла международное сотрудничество в сфере кибербезопасности: в Брюссель были направлены атташе по кибербезопасности, в Министерстве иностранных дел был назначен координатор по международной кибербезопасности, в представительстве технического посла Дании в Силиконовой долине был назначен советник по кибербезопасности, а также было осуществлено присоединение к Центру передового опыта по совместной киберзащите при Организации Североатлантического договора в Таллине. Это позволило Дании активизировать свое участие в межгосударственных киберфорумах, которые проводят, например, Организация Объединенных Наций, Европейский союз, Организация Североатлантического договора и Организация по безопасности и сотрудничеству в Европе. Дания также является активным членом Группы сотрудничества в области сетевой информационной безопасности и сети групп реагирования на инциденты, связанные с компьютерной безопасностью, а также членом правления Агентства Европейского союза по кибербезопасности. Участвуя в работе этих форумов, Дания последовательно содействует формированию глобального, открытого, стабильного, мирного и безопасного киберпространства.

Кроме того, Дания сыграла активную роль в разработке инструментария Европейского союза по вопросу сетей 5G. Цель инструментария — определить согласованный европейский подход к использованию сетей 5G на основе реализации общего пакета мер, направленных на снижение основных рисков для кибербезопасности сетей 5G.

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 по достижениям в сфере

информатизации и телекоммуникаций в контексте международной безопасности. К вопросам поведения государств в киберпространстве применяется существующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека. Кроме того, Дания подчеркивает, что 11 добровольных и не имеющих обязательной силы норм ответственного поведения государств, сформулированных в докладах Группы правительственных экспертов 2015 года, важны в качестве дополнения к имеющему обязательную силу международному праву.

Несмотря на наши совместные усилия, уровень способности и готовности государственных и негосударственных субъектов осуществлять в киберпространстве вредоносную деятельность продолжает увеличиваться. Это должно вызывать в мире озабоченность. Вредоносная деятельность в киберпространстве может представлять собой действия, являющиеся противоправными по международному праву, а также может дестабилизировать обстановку и создавать опасность эскалации. Дания по-прежнему преисполнена решимости предотвращать, пресекать и отвечать на злонамеренные действия и стремится к расширению международного сотрудничества в этой области. Дания поддерживает призыв Европейского союза к тому, чтобы международное сообщество укрепляло 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

Как уже упоминалось, Дания признает, что киберпространство открывает огромные возможности для повышения благосостояния, ускорения устойчивого экономического роста и улучшения качества жизни наших граждан. Тем не менее наша зависимость от цифровых решений также создает определенные проблемы.

Дания обеспокоена тем, что государственные и негосударственные субъекты активизируют вредоносную деятельность в киберпространстве и что оно используется для посягательств на интеллектуальную собственность. Такие действия угрожают экономическому росту и стабильности международного сообщества.

Никогда еще потребность в открытом, безопасном, стабильном, доступном и мирном киберпространстве не была столь очевидна, как во время пандемии коронавирусной болезни (COVID-19). Информационно-коммуникационные технологии (ИКТ) позволяют осуществлять общение, сотрудничество и обмен знаниями, которые необходимы миру для борьбы с пандемией.

Тем не менее во время нынешнего кризиса, вызванного коронавирусной инфекцией (COVID-19), мы стали свидетелями того, что злоумышленники будут использовать любую возможность — даже глобальную пандемию. В частности, они препятствуют функционированию критически важной инфраструктуры, включая больницы, необходимые для борьбы с пандемией. Эти действия неприемлемы и должны быть решительно осуждены всеми государствами. Кроме того, государства должны проявлять должную осмотрительность и принимать оперативные и решительные меры против вредоносной деятельности,

осуществляемой в сфере информационно-коммуникационных технологий (ИКТ) с их территории.

Как международное право применяется к использованию 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 ясно заявило о том, что тема киберпространства прочно укоренилась в существующем международном праве, о чем свидетельствуют консенсусные доклады групп правительственных экспертов за 2013 и 2015 годы. Дания подчеркивает, что к вопросам поведения государств в киберпространстве применяется существующее международное право, включая Устав Организации Объединенных Наций во всей его полноте, международное гуманитарное право и международное право прав человека.

Суверенитет, невмешательство и запрет на применение силы — это основополагающие принципы международного права; их нарушение со стороны государств будет представлять собой международно-противоправное деяние, в ответ на которое государства могут принимать контрмеры и добиваться возмещения в соответствии с нормами об ответственности государств. В ситуации когда сохраняются возможности для улучшения общего понимания и толкования этих основополагающих принципов, Дания поддерживает деятельность по выполнению этого итогового документа, которая осуществляется по линии Группы правительственных экспертов, Рабочей группы открытого состава по достижениям в области информатизации и телекоммуникаций в контексте международной безопасности и других международных и региональных инициатив.

Важно отметить, что принцип суверенитета не должен использоваться государствами в пределах их границ для ограничения или нарушения международных стандартов в области прав человека. Право прав человека, которое применимо к Интернету и реальной жизни, влечет за собой как негативное, так и позитивное обязательство государств соответствующим образом воздерживаться от действий, нарушающих права человека, и обязанность обеспечивать то, чтобы люди могли осуществлять свои права и свободы.

Как указано в «Военном руководстве Дании», с точки зрения применимого международного права проведение киберпространственных операций не отличается от использования обычного военного потенциала. Этот вопрос также отражен в национальном документе 2019 года «Совместная доктрина военных киберпространственных операций», в котором военным руководителям предписывается учитывать соображения о соблюдении норм 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 не является источником конфликтов, а служит инструментом для защиты гражданских лиц и ограничения несоразмерных последствий.

Существующее международное право, которое дополняют 11 добровольных норм ответственного поведения государств, не имеющих обязательной силы и сформулированных в докладе Группы правительственных экспертов

2015 года, служит государствам в качестве рамок для ответственного поведения в киберпространстве. Дания призывает все государства придерживаться этих рамок и выполнять представленные в них рекомендации.

Поскольку международная правовая база по вопросам кибербезопасности уже существует, Дания не призывает и не считает необходимым разрабатывать новые международно-правовые инструменты по кибербезопасности. При этом существуют возможности для углубления общего понимания порядка ее применения. Дания надеется, что мероприятия и рекомендации нынешней Группы правительственных экспертов и Рабочей группы открытого состава внесут вклад в подготовку уточнений и тем самым будут содействовать столь необходимому соблюдению государствами своих обязательств, что в конечном итоге будет 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 стимулировать работу, неоднократно одобренную Генеральной Ассамблеей, в частности в ее резолюции 70/237, и дальнейшее осуществление этих согласованных норм и мер по укреплению доверия, которые играют важную роль в предотвращении конфликтов.

Огромное значение имеют нормы, правила и принципы ответственного поведения государств, дополняющие обязательное международное право и сформулированные в ряде докладов Группы правительственных экспертов в 2010, 2013 и 2015 годах. 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.

Франция

[Подлинный текст на французском языке]
[29 мая 2020 года]

Франция приветствует возможность отреагировать на резолюцию 74/28 Генеральной Ассамблеи, озаглавленную «Поощрение ответственного поведения государств в киберпространстве в контексте международной безопасности», и хотела бы представить нижеследующую информацию.

1. Общая оценка вопросов кибербезопасности

Прежде всего Франция хотела бы напомнить, что она не использует термин «информационная безопасность», предпочитая термины «безопасность информационных систем» или «кибербезопасность». Франция не считает информацию как таковую потенциальным источником уязвимости. К тому же термин «кибербезопасность» является более точным, поскольку он относится к способности информационной системы сохранять устойчивость перед лицом событий, которые возникают в киберпространстве и могут угрожать наличию, целостности или конфиденциальности хранящихся, обрабатываемых или передаваемых данных и соответствующих услуг, которые предоставляются или становятся доступными благодаря таким системам.

Франция считает, что цифровое пространство должно оставаться пространством свободы, обмена идеями и роста, способствуя процветанию и прогрессу нашего общества. Это открытое, безопасное, стабильное, доступное и

мирное киберпространство, которое открывает экономические, политические и социальные возможности и развитие которого Франция поощряла в течение последних трех десятилетий, сегодня находится под угрозой из-за появления новых вредоносных видов деятельности. Действительно, специфика цифрового пространства (в частности, относительная анонимность, низкая стоимость и легкость доступа к вредоносным инструментам, существование факторов уязвимости и распространение определенных инструментов) позволяет ряду субъектов осуществлять шпионаж, незаконную торговлю, дестабилизацию и саботаж. Хотя некоторые незначительные угрозы не имеют отношения к национальной безопасности, а представляют собой скорее одну из форм преступности, использование таких инструментов против государственных информационных систем, критически важной инфраструктуры или предприятий может иметь серьезные последствия.

Вопрос кибербезопасности составляет сегодня неотъемлемую часть стратегий власти и соотношения сил, которые регулируют международные отношения; этот вопрос имеет приоритетный и первостепенный политический характер. Франция считает, что государства должны сохранить свою монополию на законное насилие как в киберпространстве, так и в других сферах. Однако развитие цифровых технологий в качестве нового инструмента и новой сферы конфликтов приводит к тому, что частный сектор, в том числе ряд системных субъектов, играют важнейшую роль и несут беспрецедентную ответственность в деле поддержания международного мира и безопасности.

2. Усилия Франции, предпринимаемые в сфере кибербезопасности на национальном и международном уровнях, и мнения Франции по содержанию концепций, упомянутых в докладах Группы правительственных экспертов

Уже несколько лет Франция предпринимает активные политико-дипломатические усилия, направленные на сохранение, развитие и поощрение открытого, безопасного, стабильного, доступного и мирного киберпространства и на борьбу с угрозами международной стабильности и безопасности.

Работа первых пяти групп правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в которых принимала участие Франция, позволила добиться прогресса по таким вопросам, как определение общих принципов, коллективное понимание киберпространства, в частности в сфере международного сотрудничества, и стандартов, а также понимание путей применения международного права.

Действия, предпринятые Францией в области международного сотрудничества, укрепления потенциала и поощрения и разработки мер по укреплению доверия

Франция содействует развитию международного сотрудничества в области кибербезопасности на двустороннем, европейском и международном уровнях.

Что касается деятельности на уровне Европейского союза, то в целях укрепления кибербезопасности европейского пространства Франция содействует разработке механизма добровольного сотрудничества, направленного на предотвращение и урегулирование инцидентов. Этот механизм опирается, в частности, на разработку общих оперативных норм и процедур межпартнерского сотрудничества, которые проверяются в ходе общеевропейских учений. Кроме того, Франция участвовала в разработке «кибернетического инструментария», который служит европейским странам как механизм совместного

дипломатического реагирования на кибератаки и опирается на меры по предупреждению, сотрудничеству, стабилизации и реагированию на кибератаки, включая ограничительные меры. Франция также участвует в формировании сети “CyCLONe”, которая позволит наладить оперативное сотрудничество между национальными агентствами по вопросам европейской кибербезопасности в случае возникновения кризисов в киберпространстве, а также вовлечена в проведение совместных учений в целях подготовки к подобным кризисам в дополнение к сотрудничеству между их центрами по мониторингу, предупреждению и реагированию на кибератаки.

Что касается деятельности в рамках Организации Североатлантического договора (НАТО), то в июне 2016 года на саммите в Варшаве по инициативе Франции союзники приняли обязательство по вопросам кибероборонны. В рамках этого обязательства каждое государство — член НАТО выделит соответствующую долю ресурсов на укрепление своего потенциала в области кибероборонны, что позволит также повысить общий уровень безопасности Альянса.

Принимая активное участие в деятельности неофициальной рабочей группы по кибербезопасности при Организации по безопасности и сотрудничеству в Европе (ОБСЕ), Франция продолжает содействовать осуществлению 16 мер по укреплению доверия, разработанных ОБСЕ в целях решения существующих в этой области проблем. В частности, наряду с другими государствами-участниками Франция в экспериментальном порядке осуществляет меру по укреплению доверия, касающуюся обеспечения безопасности критически важной инфраструктуры.

Франция также считает, что многие вопросы кибербезопасности должны решаться на основе многосторонности и с учетом роли и конкретных обязанностей негосударственных субъектов. В инициативе «Парижский призыв», которая была запущена в 2018 году, Франция подчеркнула «необходимость укрепления многостороннего подхода». Франция считает, что гражданское общество, научные круги, частный сектор и техническое сообщество обладают навыками и ресурсами, необходимыми для определения ряда аспектов политики кибербезопасности. Инициатива «Парижский призыв к укреплению доверия и безопасности в киберпространстве»[2], которая была представлена президентом Республики на Форуме по вопросам регулирования Интернета, состоявшемся 12 ноября 2018 года в Организации Объединенных Наций по вопросам образования, науки и культуры, отражает активную роль Франции в деле содействия формированию безопасного, стабильного и открытого киберпространства. Сегодня инициатива «Парижский призыв», которая представляет собой крупнейшую в мире многостороннюю инициативу в области кибербезопасности, поддерживается 78 государствами и более чем 1000 негосударственными субъектами. Она призвана содействовать соблюдению ряда основополагающих принципов регулирования цифрового пространства, таких как соблюдение международного права и прав человека в киберпространстве, ответственное поведение государств, государственная монополия на законное насилие и признание конкретных обязанностей частных субъектов.

Франция также поддержала деятельность Глобальной комиссии по стабильности в киберпространстве, которая готовит предложения в отношении норм и стратегий, направленных на укрепление международной безопасности и стабильности, и определяет параметры ответственного поведения государств в

[2] Имеется на веб-сайте по адресу: https://pariscall.international/fr.https://pariscall.international/fr

киберпространстве. Доклад, содержащий выводы Комиссии, был представлен на втором Парижском форуме мира.

В рамках Группы двадцати Франция стремится к тому, чтобы в ходе осуществляемой работы, как предусмотрено в инициативе «Парижский призыв», учитывались основополагающие вопросы конкуренции в сфере цифровой экономики и новые методы регулирования и управления в сфере цифровой безопасности.

Наконец, Франция также участвовала в деятельности Организации экономического сотрудничества и развития (ОЭСР). В настоящее время она председательствует в Рабочей группе ОЭСР по безопасности и конфиденциальности в цифровой экономике и хотела бы заниматься такими вопросами, как ответственность частных субъектов, обеспечение безопасности продуктов и услуг и ответственное раскрытие информации о факторах уязвимости.

В плане укрепления потенциала Франция считает, что по причине тесной взаимосвязи сетей и общества всеобщая кибербезопасность будет обеспечена только в случае способности каждого государства уверенно защищать свои информационные системы. Таким образом, действуя на двусторонней основе или в рамках многосторонних инициатив, она прилагает усилия для укрепления потенциала своих партнеров в области кибербезопасности. Кроме того, такие усилия по укреплению сотрудничества выгодны всем сторонам: они позволяют получать передовые знания в рамках взаимодействия с партнерами и перенимания их опыта, обогащать друг друга знаниями и опытом и укреплять доверие между заинтересованными сторонами. В последние годы Франция также направляла международных технических экспертов по кибербезопасности, которые работали в составе сил внутренней безопасности стран-партнеров. Например, Франция продолжает сотрудничать с Сенегалом в обеспечении работы Национальной школы кибербезопасности, которая была открыта в Дакаре в конце 2018 года и деятельность которой направлена на решение региональных задач. Цель этого проекта — проводить краткосрочные курсы, которые могут адаптироваться и служат для подготовки специалистов по кибербезопасности и высокопоставленных чиновников, прежде всего из стран Западной Африки.

Важный опыт в деле определения стандартов ответственного поведения

Опираясь на положения своей национальной доктрины, Франция разработала ряд административно-законодательных механизмов для применения норм поведения, рекомендованных в докладах Группы правительственных экспертов, в частности в докладе 2015 года (A/70/174). Нижеприводимая информация, не будучи исчерпывающей, призвана проиллюстрировать, как Франция стремится соблюдать эти нормы.

> Норма a): В соответствии с целями Устава Организации Объединенных Наций, в том числе касающимися поддержания международного мира и безопасности, государства должны сотрудничать в разработке и осуществлении мер по укреплению стабильности и безопасности в использовании ИКТ и предупреждению совершения действий в сфере ИКТ, признанных вредоносными или способных создать угрозу международному миру и безопасности.

В свете этой нормы Франция приняла ряд мер, в частности доработала национальную стратегию кибербезопасности, в которой основное внимание уделяется вопросам обороны, предотвращения, жизнестойкости и сотрудничества. В стратегическом обзоре по вопросам кибербезопасности, опубликованном

в 2018 году[3], сформирована доктрина антикризисного управления и уточнены наши цели. В ней подтверждается французская модель, в которой проводится различие между учреждениями, отвечающими за наступательный потенциал, и учреждениями, решающими оборонительные задачи. В этом обзоре также решительно подтверждается дипломатическая цель, заключающаяся в укреплении доверия и стабильности в киберпространстве.

Кроме того, Франция налаживает с различными партнерами двусторонний стратегический диалог по вопросам кибербезопасности. Как упоминалось выше, она также принимает активное участие в работе многих форумов по региональному и международному сотрудничеству и координации.

Франция также признала, что она способна проводить оборонительные и наступательные военные операции в киберпространстве, с тем чтобы обеспечить свой национальный суверенитет в строгом соответствии с национальным и международным правом. В целях обеспечения транспарентности и последовательности своих действий в 2019 году она сделала свои доктрины доступными для максимально широкого круга людей, опубликовав ряд документов, в частности материалы о военной доктрине наступательной кибервойны, а также официальный документ по международному праву, применяемому к военным операциям в киберпространстве. Это стремление прояснить и опубликовать стратегию Франции должно привести к снижению уровня недопонимания и неопределенности, тем самым способствуя укреплению духа доверия и прозрачности в киберпространстве. Франция призывает другие государства сделать то же самое.

Норма b): Государства должны изучить в случае инцидентов в сфере ИКТ всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности в ИКТ-среде, а также характер и масштабы ответственности.

Франция разработала следующие процедуры урегулирования кризисов, а также национальные структуры и стратегии на случай возникновения технологических инцидентов:

– Межведомственная антикризисная группа, которая будет развернута в случае крупного кризиса;

– Координационный центр по борьбе с кризисами в киберпространстве, который проводит свои заседания каждый месяц и состоит из оперативно-технической группы и межведомственно-стратегической группы высокого уровня. В случае возникновения киберинцидентов члены группы стратегического уровня анализируют киберинциденты в более широком контексте. Они оценивают их последствия и могут рассмотреть вопрос о возложении ответственности. Франция считает, что право о возможном возложении ответственности за нападение и решение обнародовать информацию об этом относятся к числу суверенных прерогатив.

Франция разработала средства для оценки инцидентов, в том числе с использованием шкалы тяжести, с тем чтобы помочь руководителям проводить анализ и принимать меры. При определении тяжести инцидентов Франция учитывает, в частности, их последствия с точки зрения следующих факторов:

– интересы государства, его суверенитет и демократия;

– внутренняя и гражданская безопасность;

[3] Имеется на веб-сайте по адресу www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3-publication.pdf.

– население и окружающая среда;

– экономика.

Могут учитываться и другие критерии (умысел, опасность, возложение ответственности, объем и повторяемость).

Норма c): Государства не должны заведомо позволять использовать свою территорию для совершения международно-противоправных деяний с использованием ИКТ.

Чтобы не допустить использования своей территории для совершения злонамеренных действий, Франция предприняла следующие шаги:

– вменение в обязанность операторам национальной критически важной инфраструктуры (закон № 2013-1168) и операторам основных услуг (закон № 2018-133) усилить безопасность их информационно-коммуникационных систем («жизненно важные операторы»);

– установление уголовной ответственности (статья 323-1 уголовного кодекса) за несанкционированное проникновение в системы информационной безопасности третьих сторон;

– повышение способности Национального агентства по безопасности информационных систем выявлять киберинциденты, затрагивающие операторов критически важной инфраструктуры (закон № 2018-607);

– поощрение ответственного раскрытия информации о степени уязвимости: лица, сообщающие Национальному агентству по безопасности информационных систем об уязвимости цифрового продукта или услуги, защищены от возможного судебного преследования (закон № 2016-1321).

Норма d): Государства должны рассмотреть вопрос о наилучших путях сотрудничества в целях обмена информацией, оказания взаимопомощи, преследования лиц, виновных в террористическом и преступном использовании ИКТ, а также осуществлять другие совместные меры по противодействию таким угрозам. При необходимости рассмотреть вопрос о разработке новых мер в этой сфере.

В дополнение к представленной в нашем ответе информации о сотрудничестве Франция разработала ряд мер по развитию сотрудничества с партнерами для предотвращения использования информационных технологий в преступных и террористических целях, в частности путем присоединения к Конвенции о киберпреступности (Будапештская конвенция) и поддержки Крайстчерчского призыва к ликвидации в Интернете материалов, пропагандирующих терроризм и насильственный экстремизм.

В техническом плане Национальное агентство по безопасности информационных систем продолжает налаживать партнерские отношения с аналогичными учреждениями из многих стран, с тем чтобы содействовать обмену важными данными, такими как информация о факторах уязвимости или недостатках продуктов и услуг. Кроме того, действующий при Агентстве Правительственный центр мониторинга, оповещения и реагирования на компьютерные атаки активно участвует в работе нескольких многосторонних сетей (Форум групп оперативного реагирования и обеспечения безопасности, Общеевропейская структура групп реагирования на инциденты информационной безопасности, Европейское объединение правительственных групп реагирования на инциденты информационной безопасности и Сеть групп реагирования на инциденты информационной безопасности Европейского союза), через которые он поддерживает

контакты с центрами мониторинга, оповещения и реагирования на компьютерные атаки во всем мире.

> Норма e): Государства в процессе обеспечения безопасного использования ИКТ должны соблюдать положения резолюций Совета по правам человека 20/8 и 26/13 о поощрении, защите и осуществлении прав человека в Интернете и резолюций Генеральной Ассамблеи 68/167 и 69/166 о праве на неприкосновенность личной жизни в эпоху цифровых технологий, чтобы обеспечить всестороннее уважение прав человека, включая право свободно выражать свое мнение.

Франция придает огромное значение принципам, согласно которым права человека должны соблюдаться и поощряться в Интернете и люди должны пользоваться в Интернете теми же правами, что и в реальной жизни. С 1978 года Национальная комиссия по информационным технологиям и свободам является органом, ответственным за обеспечение соблюдения в стране прав человека и основных свобод, в частности прав на неприкосновенность частной жизни и свободу выражения мнений.

Кроме того, Франция внесла вклад в принятие европейских нормативных актов, в которых учитывается необходимость обеспечивать конкурентоспособность и использовать потенциал цифровых технологий в условиях обеспечения защиты граждан и предприятий государств-членов (право на неприкосновенность частной жизни и защиту персональных данных, защита критически важной инфраструктуры и борьба с распространением террористических материалов в Интернете). Об этом желании свидетельствует то, что был принят регламент (ЕС) 2016/679 Европейского парламента и Совета от 27 апреля 2016 года «О защите физических лиц при обработке персональных данных и о свободном обращении таких данных», в 2016 году была одобрена директива (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года «О мерах по достижению общего высокого уровня безопасности сетевых и информационных систем», а также было поддержано расширение полномочий Агентства Европейского союза по кибербезопасности. Наконец, Франция стремится к тому, чтобы в рамках промышленной политики Европейского союза поддерживалась передовая научно-исследовательская деятельность, которая содействовала бы внедрению надежных и независимым образом проверенных цифровых технологий и услуг. Франция также активно участвовала в разработке руководящих принципов Европейского союза о свободе выражения мнений, которые были приняты Советом 12 мая 2014 года и направлены на обеспечение этой свободы в сети Интернет и реальной жизни.

В Совете Европы Франция поддерживает действия по защите прав человека в Интернете. Например, Франция поддержала принятие «Руководства по правам человека для пользователей Интернета», которое было разработано в апреле 2014 года Комитетом министров Совета Европы и в котором особое внимание уделяется свободе выражения мнений, доступу к информации, свободе собраний, праву на неприкосновенность частной жизни, защите персональных данных и защите от киберпреступлений, а их соблюдение должно в одинаковой степени обеспечиваться в сети Интернет и в реальной жизни.

В Организации Объединенных Наций Франция поддержала принятие всех резолюций Совета по правам человека о поощрении защиты и осуществлении прав человека в Интернете и резолюции Генеральной Ассамблеи о праве на неприкосновенность личной жизни в цифровой век.

На Парижском форуме мира, состоявшемся в ноябре 2018 года, президент Эммануэль Макрон и 11 других глав государств и правительств также объявили

о начале осуществления межправительственной инициативы в области информации и демократии с опорой на работу, уже проделанную по этому вопросу неправительственной организацией «Репортеры без границ». В настоящее время эта инициатива осуществляется под эгидой Альянса за многосторонность, учрежденного Францией и Германией.

> Норма f: Государства не должны заведомо осуществлять и поддерживать деятельность в сфере ИКТ, если такая деятельность противоречит их обязательствам по международному праву, наносит преднамеренный ущерб критически важной инфраструктуре или иным образом препятствует использованию и функционированию критически важной инфраструктуры для обслуживания населения.

В духе этой нормы, как уже упоминалось выше, Франция установила уголовную ответственность (статья 323-1 уголовного кодекса) за несанкционированное проникновение в автоматизированные системы обработки данных третьих сторон.

Кроме того, в открытых концептуальных материалах, включая официальный документ 2019 года под заголовком «Международное право, применяемое к операциям в киберпространстве», Франция четко установила, что международное гуманитарное право в полной мере применяется к кибероперациям, проводимым в контексте вооруженных конфликтов и в связи с ними, о чем будет более подробно разъяснено в разделе о международном праве.

> Норма g: Государства должны принимать надлежащие меры для защиты своей критически важной инфраструктуры от угроз в сфере ИКТ, принимая во внимание резолюцию 58/199 Генеральной Ассамблеи о создании глобальной культуры кибербезопасности и защите важнейших информационных инфраструктур и другие соответствующие резолюции.

Чтобы содействовать усилению защиты критически важной инфраструктуры, Франция разработала, как указывалось выше, нормативную базу для защиты такой инфраструктуры, обязав жизненно важных операторов повысить уровень безопасности используемых ими критически важных информационных систем — информационных систем, имеющих жизненно важное значение (закон № 2013-1168 от 18 декабря 2013 года), а также расширив сферу полномочий Национального агентства по безопасности информационных систем и повысив его способность выявлять инциденты. Жизненно важные операторы должны также активизировать усилия по обеспечению безопасности и использовать одобренные Агентством системы обнаружения. Франция поощряет сотрудничество между государственным и частным секторами, направленное на усиление защиты критически важной инфраструктуры и определение пригодных эффективных рамок.

> Норма h): Государства должны удовлетворять соответствующие просьбы об оказании помощи, поступающие от других государств, критически важная инфраструктура которых становится объектом злонамеренных действий в сфере ИКТ. Государства также должны удовлетворять соответствующие просьбы о смягчении последствий злонамеренных действий в сфере ИКТ, направленных против критически важной инфраструктуры других государств, если такие действия проистекают с их территории, принимая во внимание должным образом концепцию суверенитета.

Для соблюдения этой нормы Франция, например, создала сеть доверительного сотрудничества, осуществляемого в рамках технического партнерства на уровне Национального агентства по безопасности информационных систем; эта сеть, в частности, позволяет устанавливать контакты между центрами по

мониторингу, предупреждению и реагированию на кибератаки через постоянных координаторов.

В целях налаживания антикризисного управления Франция также создала постоянный межведомственный механизм, предназначенный для анализа угроз, подготовки и координации и функционирующий в виде координационного центра по борьбе с кризисами в киберпространстве. Благодаря этому центру различные службы, в частности, могут беспрепятственно обмениваться информацией, с тем чтобы улучшить координацию на национальном уровне и удовлетворить эти потребности.

В соответствии с Бухарестской конвенцией Франция также создала сеть координаторов, которая функционирует на круглосуточной основе и позволяет блокировать данные.

В рамках ОБСЕ Франция обязалась ввести в действие ряд координационных центров (мера по укреплению доверия № 8, решение № 1106 Постоянного совета ОБСЕ) и поддерживать различные усилия к тому, чтобы каждое государство создавало соответствующие каналы обмена информацией (мера по укреплению доверия № 13, решение № 1202 Постоянного совета).

> Норма i): Государства должны принимать разумные меры для обеспечения целостности каналов поставки, чтобы конечные пользователи могли быть уверены в безопасности продуктов ИКТ. Государства должны стремиться предупреждать распространение злонамеренных программных и технических средств в сфере ИКТ и использование скрытых вредоносных функций.

Франция поощряла разработку норм и стандартов для этой отрасли, в частности в рамках инициативы «Парижский призыв». Она также содействовала началу международной работы по этой теме на различных форумах, главным образом в рамках Целевой группы по цифровой экономике при Группе 20 и ОЭСР.

Франция также содействовала использованию принципов сертификации третьими сторонами под эгидой Национального агентства по безопасности информационных систем, с тем чтобы на рынке обеспечивался наивысший уровень безопасности. В рамках Агентства этот процесс осуществляется на экспериментальной основе Национальным центром сертификации. Франция также содействовала внедрению таких сертификатов на уровне Европейского союза.

Чтобы активизировать борьбу с распространением вредоносных средств и технологий, Франция также поддержала включение программного обеспечения для несанкционированного доступа в список предметов двойного назначения Вассенаарских договоренностей.

> Норма j): 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 возможные угрозы для ИКТ и зависящей от ИКТ инфраструктуры.

Как указывалось выше, Франция приняла различные меры, позволяющие ответственно раскрывать информацию о факторах сетевой уязвимости, и наладила сотрудничество на техническом уровне через Национальное агентство по безопасности информационных систем, которое регулярно обменивается информацией о факторах уязвимости и имеющихся решениях со своими коллегами и партнерами.

Норма k): Государства не должны заведомо осуществлять и поддерживать деятельность, призванную нанести ущерб информационным системам уполномоченных групп экстренной готовности к компьютерным инцидентам (также именуемым группами готовности к компьютерным инцидентам или группами готовности к инцидентам в сфере кибербезопасности) другого государства. Государство не должно использовать уполномоченные группы экстренной готовности к компьютерным инцидентам для осуществления злонамеренной международной деятельности.

Закон Годфрана (закон № 88-19 от 5 января 1988 года) о компьютерном мошенничестве — это первый французский закон, предусматривающий наказание за преступления и взломы в компьютерной сфере. Он устанавливает уголовную ответственность в отношении лиц, которые мошенническим образом получают полный или частичный доступ к автоматизированной системе обработки данных или сохраняют свое присутствие в рамках этой системы.

Французская модель управления, в соответствии с которой наступательные возможности отличаются от оборонительных возможностей и задач, обеспечивает соблюдение этого принципа. Задачи Правительственного центра мониторинга, оповещения и реагирования на компьютерные атаки заключаются, в частности, в координации и расследовании мер реагирования на киберинциденты в интересах не только французского правительства, но и операторов критически важных объектов инфраструктуры и основных услуг, определенных в законодательстве, путем оказания этим операторам помощи в установлении необходимого уровня защиты, выявлении факторов уязвимости в сетях и системах, организации реагирования на инциденты с помощью партнеров, если это необходимо, и участия в работе пользующейся доверием сети центров реагирования на инциденты в области компьютерной безопасности.

Исследование по вопросу о применении международного права, включая Устав Организации Объединенных Наций, в киберпространстве: очередной принцип, признанный Группой правительственных экспертов

Франция считает, что работа по созданию коллективной системы кибербезопасности может осуществляться только на основе соблюдения существующих норм международного права. По мнению Франции, на данном этапе не нужно разрабатывать новый юридически обязательный международный документ, посвященный проблемам кибербезопасности. В киберпространстве, как и в других областях, применяется и должно соблюдаться действующее международное право.

Как Группа правительственных экспертов заключила в своем докладе 2013 года, принципы и нормы международного права применяются к поведению государств в киберпространстве. Хотя киберпространство имеет особенности (анонимность и роль частных субъектов), международное право обеспечивает необходимые средства для ответственного регулирования поведения государств в этой среде.

Принцип суверенитета применяется к киберпространству. В этой связи Франция подтверждает, что в пределах своей территории и юрисдикции и в рамках своих обязательств по международному праву она осуществляет свой суверенитет в отношении информационных систем, людей и деятельности в киберпространстве. Несанкционированное проникновение в французские системы, которое влечет за собой оказание воздействия и осуществляется на французской территории с помощью наступательных киберсредств государственным учреждением или негосударственным субъектом, действующим по указанию или под

контролем какого-либо государства, может представлять собой посягательство на суверенитет.

Масштаб мер, которые могут быть приняты государствами в ответ на возможную кибератаку против них, зависит от серьезности ее последствий. Таким образом, кибероперация может рассматриваться как применение силы, запрещенное в соответствии с пунктом 4 статьи 2 Устава Организации Объединенных Наций. Преодоление порога, связанного с применением силы, зависит не от используемых киберсредств, а от последствий кибероперации. Если они аналогичны последствиям, возникающим в результате применения обычных вооружений, то кибероперация может рассматриваться как применение силы. Ввиду этого Франция считает, что серьезная компьютерная атака, которая совершена государством или негосударственными субъектами, действующими под контролем государства или по его указанию, — когда она достигает по своим масштабам или последствиям достаточно серьезный уровень (например, массовая гибель людей, значительный физический ущерб, неисправности в работе критически важной инфраструктуры со значительными последствиями) — может представлять собой «вооруженное нападение» по смыслу статьи 51 Устава Организации Объединенных Наций и тем самым служить основанием для требования об осуществлении законной обороны. Такая законная оборона может осуществляться обычными или кибернетическими средствами при условии соблюдения принципов необходимости и соразмерности. Квалификация компьютерной атаки как «вооруженного нападения» по смыслу статьи 51 Устава осуществляется в рамках политического решения, принимаемого по каждому конкретному случаю с учетом установленных международным правом критериев.

Франция также признает, что международное гуманитарное право в полной мере применяется к кибероперациям, проводимым в контексте вооруженных конфликтов и в связи с ними. В настоящее время наступательные кибероперации проводятся в сочетании с обычными военными операциями.

Несмотря на свой нематериальный характер, эти операции по-прежнему подчинены принципу географического охвата применения международного гуманитарного права, то есть их последствия ограничиваются территорией государств-сторон международного вооруженного конфликта или территорией, на которой ведутся военные действия в рамках немеждународного вооруженного конфликта. В ходе наступательных операций, проводимых французскими вооруженными силами в области электронной борьбы, соблюдаются следующие принципы международного гуманитарного права:

– принцип проведения различия между гражданскими и военными объектами. В силу этого запрещено совершать кибератаки, не направленные против конкретного военного объекта или осуществляемые с помощью кибероружия, которое нельзя применять против конкретного военного объекта. В этой связи некоторые данные контента, несмотря на их нематериальный характер, могут представлять собой гражданские объекты, охраняемые в соответствии с международным гуманитарным правом. Кроме того, в соответствии с этим принципом должно проводиться различие между комбатантами или членами организованных вооруженных групп и гражданскими лицами. Кибератаки не должны быть направлены против гражданского населения как такового или гражданских лиц, за исключением случаев — и только в ходе — их прямого участия в военных действиях. Во время вооруженного конфликта любой киберкомбатант-военнослужащий одной из сторон в конфликте, любой член организованной вооруженной группы, совершающий кибератаки на противника, или любое гражданское лицо, принимающее прямое участие в военных действиях с помощью киберсредств,

могут подвергнуться нападению с использованием обычных или кибернетических средств;

– принцип соразмерности и принцип предосторожности. При проведении этих операций следует проявлять постоянную осмотрительность, обеспечивая защиту населения и гражданского имущества от последствий боевых действий. Сопутствующий ущерб не может превышать ожидаемое непосредственное и конкретное военное преимущество. Чтобы в киберпространстве соблюдался принцип соразмерности, нужно учитывать все прогнозируемые последствия применения оружия — будь то прямые последствия (включая повреждение атакованной системы и прерывание обслуживания) или косвенные последствия (воздействие на инфраструктуру, функционирующую под контролем атакованной системы, и воздействие на лиц, пострадавших от сбоя или разрушения систем, изменения данных и их порчи), если эти последствия в достаточной степени вызваны нападением. В соответствии с этим принципом также запрещается применение кибероружия, которое не может контролироваться во времени и в пространстве.

Эта информация представлена в докладе о международном праве, применяемом к операциям в киберпространстве (опубликован Министерством вооруженных сил 9 сентября 2019 года), а также в открытых материалах, представленных в том же году на тему военной доктрины Франции в отношении наступательных кибероопераций.

Наконец, Франция считает важным то, что на международном уровне удалось достичь общего понимания в отношении обязанностей государств, инфраструктура которых используется в неблаговидных целях и в ущерб интересам другого государства. Цель заключается в том, чтобы уточнить порядок применения в киберпространстве принципа должной осмотрительности; этот принцип предусматривает, что каждое государство обязано «не допускать использования своей территории для совершения действий, нарушающих права других государств»[4]. В этой связи государства не должны осознанно позволять использовать свою территорию для совершения международно-противоправных деяний с помощью киберсредств и должны принимать все обоснованно ожидаемые от них меры к тому, чтобы их территория не использовалась негосударственными субъектами для совершения таких действий. Таким образом, Франция определила параметры регулирования способности частных субъектов реагировать на инциденты в качестве важного направления работы, что могло бы содействовать ограничению масштаба действий, негативно сказывающихся на третьих сторонах, и соблюдению принципа должной осмотрительности[5]. Более глубокое понимание того, как этот принцип применяется к существующим в этой сфере проблемам, способствовало бы укреплению межгосударственного сотрудничества в целях защиты некоторых критически важных объектов инфраструктуры и прекращению крупных кибератак, совершаемых через третьи страны.

[4] *Affaire du Détroit de Corfou, Arrêt du 9 avril 1949: C.I.J. Recueil 1949*, p. 4.

[5] Такое регулирование, основополагающий принцип которого должен определять работу Группы правительственных экспертов, должно осуществляться на основе анализа рисков применения мер, которые могут самостоятельно приниматься частными субъектами в ответ на тот или иной инцидент.

Грузия

[Подлинный текст на английском языке]
[29 мая 2020 года]

Правительство Грузии, содействуя поиску безопасных, устойчивых к негативным воздействиям, хорошо защищенных и надежных технологических решений в области электронного правительства и развитию информационного общества в целом, внимательно изучает все возможности для выполнения рекомендаций Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в отношении поощрения ответственного поведения государств в киберпространстве. Грузия стремится активно содействовать соблюдению принципов и рекомендаций Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и разрабатывать для этого специальные национальные механизмы.

Ниже кратко излагается новая важная информация о развитии кибербезопасности и информационной безопасности в Грузии и усилиях, прилагаемых на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству.

Грузия по-прежнему привержена развитию своей концепции кибербезопасности и достижению более высоких сравнительных показателей кибербезопасности на международном уровне. Безусловно, решение задач по укреплению кибербезопасности Грузии усложняют ее нынешние геополитические условия. 28 октября 2019 года была совершена крупномасштабная кибератака на вебсайты, серверы и другие элементы информационных систем Администрации президента Грузии, судов, различных муниципальных законодательных органов, государственных структур, организаций частного сектора и средств массовой информации. Эта кибератака была направлена против национальной безопасности Грузии и преследовала цель причинить вред грузинским гражданам и правительственным структурам, нарушив и парализовав работу различных организаций. Результаты расследования, проведенного грузинскими властями, вкупе с информацией, собранной благодаря сотрудничеству с нашими партнерами, позволили сделать вывод о том, что эта кибератака была спланирована и совершена Главным управлением Генерального штаба Вооруженных сил Российской Федерации. Вышеупомянутый инцидент подтверждает важность усилий правительства Грузии по укреплению кибербезопасности на национальном уровне и вновь свидетельствует о необходимости укрепления международного партнерства по вопросам кибербезопасности.

Грузия направляет все свои ресурсы на то, чтобы стать более сильной, безопасной и защищенной страной в киберпространстве. В частности, правительство Грузии стремится к тому, чтобы каждая целевая группа информационного общества обладала необходимым уровнем знаний и опыта для борьбы с киберугрозами. Грузинская модель управления предоставляет государственным и частным организациям возможность коллективно или самостоятельно обеспечивать кибербезопасность страны и соответствующую стабильность путем совместного использования ресурсов. Кроме того, Грузия пользуется международным признанием и поддержкой со стороны своих международных партнеров, в свою очередь, являясь для них надежным партнером в области кибербезопасности.

Правительство Грузии активно стремится к созданию открытого, безопасного и защищенного киберпространства. Обеспечение кибербезопасности относится к числу стратегических направлений политики правительства Грузии в области национальной безопасности, и на политическом уровне большое

внимание уделяется дальнейшему развитию и укреплению потенциала противодействия в данной сфере. Правительство видит свою исключительную роль в создании благоприятной среды для функционирования информационного общества, цифровой экономики и электронного управления в стране; правительство берет на себя ответственность за формирование соответствующей стратегической, организационно-институциональной и нормативно-правовой базы, которая поможет как гражданам, так и государственному и частному сектору безопасно и надежно осуществлять свою деятельность в цифровой среде при условии их безопасного поведения в интернет-пространстве.

Видное место в политической повестке дня правительства Грузии занимает укрепление двустороннего, регионального и международного сотрудничества в области кибербезопасности. Грузия служит хорошим примером партнерства на региональном и международном уровнях и в многосторонних форматах (Европейский союз, Организация Североатлантического договора (НАТО), Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Организация Объединенных Наций, Восточное партнерство, Совет Европы, Агентство Европейского союза по сотрудничеству правоохранительных органов, Международная организация уголовной полиции, Европейский полицейский колледж, Европейское агентство по кибербезопасности). Грузия активно участвует в международных проектах и совещаниях, посвященных вопросам кибербезопасности.

В последние годы был предпринят ряд инициатив в области сотрудничества и партнерства, о которых говорится ниже:

- шаги по укреплению кибербезопасности, предпринимаемые Грузией в последнее десятилетие, приносят положительные результаты, а проведенные реформы и текущие процессы положительно оцениваются на международном уровне. Грузия занимает видное место и входит в число лидеров по уровню развития в области кибербезопасности среди стран Восточного партнерства и потому играет роль регионального организационного центра при проведении различных мероприятий по наращиванию потенциала и обмену информацией и передовым опытом в области кибербезопасности для соответствующих стран.

- Сотрудничество Грузии и НАТО в области кибербезопасности находится в стадии развития. Грузия находится в активной фазе сотрудничества со странами — членами НАТО и участвует как на индивидуальной, так и на коллективной основе в различных проектах, осуществляемых под эгидой НАТО. Сюда относится также участие Грузии в стратегических или технических инициативах, связанных с учебной подготовкой. НАТО (штаб-квартира и Бюро по связи и взаимодействию) оказывает помощь грузинским структурам, занимающимся вопросами кибертехнологий, в планомерном и непрерывном повышении осведомленности различных целевых групп и проведении для них учебных мероприятий на всей территории Грузии. Грузия регулярно представляет свои достижения и инициативы в области кибербезопасности на комиссии НАТО — Грузия и тесно увязывает свою деятельность с Обязательством НАТО по киберзащите.

- Грузия и Европейский союз. В рамках пятилетней программы «Европейский союз за безопасность, подотчетность и борьбу с преступностью в Грузии» Грузия получает помощь от Европейского союза в таких областях, как борьба с киберпреступностью, кибер- и гибридными угрозами, пограничный контроль, защита гражданского населения и надзор за деятельностью сектора безопасности. Грузия укрепила сотрудничество с другими субъектами в рамках Общей политики безопасности и обороны Европейского союза, которая перекликается с его определенными на международном

уровне стратегическими целями и в целом способствует укреплению национальной безопасности Грузии, поскольку предусматривает наращивание ее оборонного потенциала.

- Грузия и ОБСЕ. Грузия высоко оценивает налаживание доверительного взаимодействия между странами-партнерами, чему способствуют меры укрепления доверия в области кибербезопасности. Грузинские контактные центры активно участвуют в программе ОБСЕ по вопросам кибербезопасности и осуществляемых в рамках этой программы инициативах.

- Правительства Грузии и Великобритании подписали Меморандум о взаимопонимании по вопросам сотрудничества в области кибербезопасности. Это было сделано в целях активизации совместной деятельности, обмена передовым опытом и более эффективного согласования подходов к различным аспектам кибербезопасности.

- Грузия и страны Восточного партнерства. Агентство по обмену данными продолжает сотрудничать со странами Восточного партнерства в рамках программы «EU4 Digital: повышение киберустойчивости в странах Восточного партнерства». Проект «Кибервосток» помогает Грузии и другим странам Восточного партнерства укрепить потенциал противодействия киберугрозам, уголовного правосудия и сбора электронных доказательств на территории стран Восточного партнерства, с тем чтобы более эффективно бороться с киберпреступностью. Основное внимание в рамках проекта уделяется совершенствованию правовой и политической базы; укреплению потенциала судебных и правоохранительных органов и межведомственного сотрудничества; и внедрению эффективных механизмов международного сотрудничества в целях укрепления взаимного доверия, в том числе между поставщиками услуг и правоохранительными органами, в таких областях, как уголовное правосудие, борьба с киберпреступностью и сбор электронных доказательств.

- Грузия продолжает укреплять региональное сотрудничество с соседними странами под эгидой Организации за демократию и экономическое развитие. В 2019 году представители Грузии приняли участие в совещаниях, состоявшихся в Киеве в штаб-квартире Организации за демократию и экономическое развитие.

- Группа реагирования на чрезвычайные ситуации в компьютерной сфере — одно из подразделений Агентства по обмену данными Министерства юстиции Грузии — подписала целый ряд меморандумов о сотрудничестве в интересах обмена знаниями и опытом с соответствующими организациями стран Европы и стран — участниц Восточного партнерства (Литвы, Румынии, Молдовы, Украины и Беларуси). Грузия активно участвует в международных киберучениях и образовательных программах, неизменно демонстрируя выдающиеся результаты.

Что касается практического аспекта, то Грузия, обладая огромными знаниями в этой области на национальном уровне, считает новейший передовой международный опыт ценным источником ориентиров и возможностей для сотрудничества в контексте укрепления стратегического, правового, институционального и инфраструктурного аспектов национальной политики, а также в процессе трансформации киберкультуры.

В 2019 году в Грузии на основе активного сотрудничества между секторальными ведомствами[6], занимающимися вопросами кибербезопасности, был разработан третий проект стратегии национальной кибербезопасности и план действий по ее реализации[7]. Координирующую роль в этом процессе играл Аппарат Совета национальной безопасности. Вместе с тем участие в реализации этого начинания приняли и соответствующие заинтересованные стороны из частного сектора, научных кругов и гражданского общества. По мере того, как Грузия стремится привести свои национальные рамки в соответствие с евроатлантическими механизмами в данной сфере, процесс стратегического развития осуществляется в значительной мере с опорой на рекомендации иностранных экспертов, а также разделяющих их взгляды консультантов на национальном уровне. Особое значение в контексте разработки стратегии национальной кибербезопасности и плана действий по ее реализации имеет помощь, оказываемая Соединенным Королевством соответствующим субъектам, занимающимся вопросами кибербезопасности в Грузии. Проект стратегии национальной кибербезопасности и плана действий по ее реализации будут утверждены правительством Грузии в течение 2020 года. Соответствующие документы будут рассмотрены постоянной межведомственной комиссией, созданной в январе 2020 года при Совете национальной безопасности и призванной координировать разработку концептуальных документов национального уровня по вопросам безопасности. Затем Совет национальной безопасности представит эти проекты документов на утверждение правительству Грузии.

Грузия продолжает укреплять нормативно-правовую базу, регулирующую вопросы киберпространства. В Грузии создана всеобъемлющая нормативно-правовая база в области информационно-коммуникационных технологий, регулирующая вопросы кибербезопасности, и принято законодательство, защищающее права отдельных лиц и организаций в цифровой среде. Соответствующие законы охватывают вопросы защиты критической информационной инфраструктуры, ответственности поставщиков интернет-услуг, обязательства по информированию об инцидентах и безопасность электронных сделок. В качестве следующего шага Грузия планирует выполнить масштабную задачу по согласованию своей законодательной базы в области кибербезопасности с Директивой Европейского союза о безопасности сетей и информационных систем. В этой связи уполномоченные ведомства в 2019 году уже инициировали процесс сотрудничества с Европейским союзом, а до конца текущего года будет подготовлено детальное техническое задание проекта двустороннего взаимодействия, цель которого заключается в оказании Грузии помощи в процессе гармонизации законодательства. По итогам осуществления этого проекта Грузия обновит свой Закон об информационной безопасности, в котором, помимо других важных аспектов, будут четко определены рамки управления кибербезопасностью, органы, ответственные за применение Директивы, а также функции и обязанности субъектов в сфере обеспечения кибербезопасности на стратегическом, оперативном и тактическом уровнях.

Кроме того, Грузия начала процесс реализации еще одной масштабной задачи, которая заключается в разработке и принятии совместимой с законодательством Европейского союза модели защиты критической информационной инфраструктуры. В течение 2019 года было проведено несколько семинаров, в ходе которых обсуждалось создание надлежащей системы выявления объектов критической инфраструктуры, функционирующей в киберпространстве, и

[6] Агентством по обмену данными (в Министерстве юстиции), Бюро по вопросам кибербезопасности (в Министерстве обороны) и Оперативно-техническим агентством (в Службе государственной безопасности).

[7] План рассчитан на трехлетний период 2020–2023 годов.

взаимодействия с их владельцами. Грузия разработала соответствующую методологию и вопросники, касающиеся объектов критической информационной инфраструктуры. В рамках этого процесса проводились обсуждения с представляющими различные сегменты и отрасли частными компаниями, относящимися к числу субъектов критической инфраструктуры.

В настоящее время ведется внедрение политики информационной безопасности и требований кибербезопасности во всех организациях, которые причисляются к субъектам критической информационной инфраструктуры. Уполномоченные государственные органы оказывают этим субъектам помощь во внедрении политики информационной безопасности и основ кибербезопасности, предоставляя рекомендации, помощь экспертов и возможности для профессиональной подготовки, а также осуществляя более многоплановые мероприятия, такие как аудит информационной безопасности, тестирование проникновения и оказание других услуг в области информационной и кибербезопасности. В учреждениях, относящихся к числу субъектов критической информационной инфраструктуры, начато осуществление различных проектов по внедрению системы управления информационной безопасностью. Эти структуры получают поддержку в таких областях, как внедрение политики информационной безопасности, решение задач по управлению активами и обзор действующей политики. Параллельно правительство устанавливает стандарты и процедуры в области информационной безопасности, принимая законы и подзаконные акты (на основе серии стандартов ИСО 27000) и организует проведение курсов профессиональной подготовки по вопросам информационной безопасности для представителей государственного и частного секторов. Следующая цель заключается в разработке и принятии правовых положений о защите критической информационной инфраструктуры, которые будут соответствовать Директиве Европейского союза о безопасности сетей и информационных систем и гарантировать применимость расширенных правовых положений, касающихся безопасности сетей и информационных систем, к защите критической информационной инфраструктуры.

Правительство Грузии успешно использует государственно-частные многосторонние платформы в качестве инструмента для налаживания доверительных отношений между всеми заинтересованными сторонами и обмена информацией и знаниями, а также для реализации новых инициатив и создания условий для участия частного сектора в процессе разработки политики и стратегий. Агентство по обмену данными, осуществляющее руководство процессом сотрудничества между государственными и частными структурами, в течение 2019 года провело целый ряд семинаров и совещаний с участием представителей финансового, энергетического и телекоммуникационного секторов, чтобы присоединиться к подготовительным консультациям в рамках процесса выявления объектов критической инфраструктуры. Заинтересованные представители частного сектора участвуют во всех основных процессах консультаций по горизонтальным проектам в рамках инициатив по разработке стратегий, политики, законодательных и нормативных актов, а также по укреплению потенциала.

Грузия на систематической и непрерывной основе проводит мероприятия для различных целевых групп по повышению информированности и профессиональной подготовке в целях повышения квалификации и совершенствования навыков в сфере кибертехнологий. При содействии государственных организаций Грузии были проведены широкомасштабные информационно-разъяснительные кампании, направленные на повышение осведомленности населения о правилах безопасного поведения в киберпространстве; также в настоящее время активно осуществляются программы обучения и переподготовки по вопросам кибербезопасности для различных целевых групп. Благодаря осуществлению

различных инициатив и образовательных программ в Грузии с каждым годом повышается уровень технологической зрелости потенциала кибербезопасности; правительство Грузии прилагало и прилагает весьма активные усилия для повышения квалификации специалистов по кибербезопасности, занятых в государственном секторе. Как следствие, они обладают высоким уровнем профессионализма и многие из них имеют признанные на международном уровне и высоко котирующиеся сертификаты таких организаций, как Институт SANS (Институт системного администрирования, аудита, сетей и безопасности), Ассоциация аудита и контроля информационных систем и Международная организация по стандартизации.

И наконец, Грузия продолжит активно участвовать в международном диалоге по вопросам регулирования Интернета, а также в осуществлении других международных инициатив, касающихся коллективной кибербезопасности.

Гондурас

[Подлинный текст на испанском языке]
[17 апреля 2020 года]

Доклад о мерах, связанных с киберпространством, в контексте международной безопасности

В рамках разработанного Международной организацией по стандартизации стандарта ИСО 27001 (международный стандарт информационной безопасности) и в интересах формирования рабочей культуры, соответствующей целям инициативы по созданию цифрового правительства, выдвинутой президентом Республики Гондурас, Национальная полиция Гондураса осуществляет ряд мер на внутреннем уровне, уделяя особое внимание ответственному использованию интернет-ресурсов в соответствии с Руководством по информационной безопасности для органов полиции, в котором четко изложена политика, принятая для защиты различных аспектов оперативной деятельности сотрудников этого ведомства и для уменьшения воздействия таких факторов, которые делают его системы уязвимыми для различного рода атак или злоумышленных действий.

Ниже перечислены некоторые из принятых Национальной полицией мер, связанных с киберпространством.

1. Разработка политики информационной безопасности

В рамках этой политики устанавливаются стандарты и руководящие принципы надлежащего использования технических средств, с тем чтобы обеспечить защищенность информационных и материальных ресурсов данного ведомства, что принципиально важно для выполнения им обязанностей, возложенных на него Конституцией, а также в целях постоянного совершенствования его деятельности путем эффективного использования передового опыта и механизмов контроля для ее регулирования и защиты при соблюдении гарантий конфиденциальности, доступности и сохранности информации в целом.

2. Учебные мероприятия

Национальная полиция Гондураса через посредство Управления полиции по вопросам связи и информационных технологий на постоянной основе проводит мероприятия по повышению осведомленности в вопросах киберпространства для сотрудников оперативных и административных подразделений, а также участвует в специализированных мероприятиях, организуя подготовку, в

частности, по таким вопросам, как интернет-травля, социальная инженерия, сфабрикованные новостные материалы, киберпреступность и кибербезопасность.

3. Использование локальной сети

Через интранет Национальной полиции, который носит название «Поливеб», осуществляется информирование сотрудников о последних тенденциях в сфере борьбы с киберпреступлениями, а также рассылка бюллетеней о важных событиях в их профессиональной области, связанных с кибербезопасностью, и распространение директив, вытекающих из руководства по информационной безопасности, в целях обеспечения компьютерной безопасности.

Этот вид внутренней связи позволяет осуществлять все внутренние операции Национальной полиции через посредство локальной сети или интранета, тем самым сводя к минимуму риск посещения ее сотрудниками неизвестных веб-сайтов, а также способствуя уменьшению нагрузки на интернет-серверы и экономии пропускной способности.

4. Урегулирование и расследование инцидентов

Группа по информационной безопасности осуществляет постоянный мониторинг сети передачи данных ведомства, выявляя факторы уязвимости и угрозы, которые могли возникнуть в компьютерных системах, используемых сотрудниками, вследствие ненадлежащего использования ими сети Интернет или при попытке обойти установленные для пользователей ограничения; одновременно с этим разрабатываются меры по расследованию и урегулированию компьютерных инцидентов в общей сети Национальной полиции. Секция управления информацией и Секция по урегулированию инцидентов Департамента по вопросам информационной безопасности занимаются анализом известных факторов уязвимости, которые могут поставить под угрозу системы ведомства и хранящуюся в них информацию. Эти факторы соответствующим образом обрабатываются и устраняются в рамках следующей официально установленной процедуры:

- внесение в инвентаризационную опись информационных активов данных о поставщике программного обеспечения, номерах версий, текущей стадии развертывания и сотрудниках, ответственных за это программное обеспечение;
- проведение анализа факторов уязвимости каждые полгода;
- обеспечение постоянного обновления информации о новых факторах уязвимости;
- определение сроков, в течение которых надлежит внести исправления и применить соответствующие средства для устранения известных факторов уязвимости;
- тестирование исправлений или патчей, устраняющих факторы уязвимости, перед развертыванием в рабочей среде.

5. Аудит

Проверка правильного использования сотрудниками полиции компьютерного оборудования, а также предоставляемого ведомством доступа к сети Интернет проводится на основе плана ежегодного аудита.

Ниже перечислены некоторые из действующих ограничений:

- запрещается установка на компьютерах программных средств для подключения к виртуальным частным сетям (VPN);
- запрещается использовать сервисы, обеспечивающие возможность анонимного посещения интернет-страниц, такие как Tor, I2P, DuckDuckGo и Whonix;
- запрещается использование социальных сетей (для отдельных подразделений предусмотрены исключения);
- запрещается использование потоковых веб-сервисов с большим объемом потребляемого сетевого трафика, таких как цифровое телевидение или сервисы просмотра видео;
- запрещается хранить личную документацию и устанавливать программное обеспечение, не имеющее отношение к рабочим обязанностям.

У информационных систем, а также серверов, сетевых устройств и другие технических средств должны иметься контрольные журналы (журналы регистрации), в которых, при наличии возможности, фиксируются следующие сведения:

- идентификаторы пользователей;
- даты и время событий;
- IP-адреса и имена устройств, с которых осуществлялись операции;
- типы операций;
- идентификаторы операций;
- просмотренные, измененные или удаленные данные;
- количество неудачных попыток соединения;
- изменения в конфигурации системы;
- изменение или отмена предоставленных пользователю привилегий;
- файлы, к которым был осуществлен доступ;
- сигналы тревоги, поступившие от систем управления доступом;
- деактивация механизмов защиты.

6. Использование антивирусных программ

Дополнительным уровнем защиты от вредоносного программного обеспечения служит действие антивирусной программы. Эта программа позволяет бороться с фишингом, защищает от «атак нулевого дня» и программ-вымогателей и постоянно уведомляет об устранении факторов уязвимости.

7. Управление межсетевым экраном

Сегментация сети и регулирование доступа к ней осуществляются с помощью межсетевого экрана — программного обеспечения для защиты сетевого периметра, которое блокирует попытки вторжения в сеть полиции и ведет учет начатых сеансов пользователей, фиксируя просмотренные веб-сайты и регистрацию пользователей в различных системах ведомства.

8. Зашифрованная связь

Что касается реагирования на чрезвычайные ситуации в области национальной безопасности, а также координации действий внутри Национальной полиции, то она располагает современной системой шифрованной радиосвязи для надежной и безопасной передачи информации.

Все вышеперечисленные меры обеспечивают более эффективную защиту внутриведомственной информации и подкрепляют усилия по предотвращению кибератак, которым системы Национальной полиции могут подвергнуться при отсутствии надлежащей защиты. В настоящее время ни одна система не является полностью защищенной, однако, осуществляя некоторые из указанных мер, мы ликвидируем факторы уязвимости в компьютерной сфере и стремимся к цифровому регулированию киберпространства путем выявления и блокирования кибератак.

Венгрия

[Подлинный текст на английском языке]
[15 мая 2020 года]

Общее понимание вопросов, касающихся киберпространства, в контексте международной безопасности

В декабре 2019 года Генеральная Ассамблея приняла резолюцию о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. В этой резолюции Ассамблея рекомендует государствам-членам продолжать информировать Генерального секретаря о своей точке зрения и оценках в отношении усилий, прилагаемых на национальном уровне для укрепления информационной безопасности и содействия международному сотрудничеству в этой области, а также в отношении содержания концепций, упомянутых в докладах Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Венгрия будет рада продолжить обсуждение на регулярной основе добровольных норм, правил и принципов ответственного поведения государств, мер укрепления доверия, а также норм международного права в рамках Первого комитета Организации Объединенных Наций и будет приветствовать формирование в дальнейшем новых групп правительственных экспертов.

В 2018 году Венгрия поддержала резолюции 73/266 и 73/27 Генеральной Ассамблеи, предусматривавшие создание, соответственно, новой Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности; учреждение этих групп стало очередным важным шагом в деле устранения угроз, связанных с использованием информационно-коммуникационных технологий (ИКТ).

Венгрия впервые принимает участие в обсуждении этих вопросов, хотя она с большим интересом следила за работой предыдущих групп правительственных экспертов, в том числе в ходе принятия в 2013 году своей первой Стратегии национальной кибербезопасности. Венгрия участвовала в совещаниях Рабочей группы открытого состава с момента ее создания. На первом совещании страну представлял ее постоянный представитель при Организации по безопасности и сотрудничеству в Европе (ОБСЕ) (по совместительству — Председатель

Неофициальной рабочей группы ОБСЕ по кибербезопасности), а на втором — координатор по вопросам кибертехнологий Министерства иностранных дел и внешнеэкономических связей. Кроме того, Венгрия активно участвует в консультациях по проекту доклада Председателя Рабочей группы открытого состава. В целом Венгрия разделяет позицию Европейского союза.

Венгрия решительно выступает за эффективную многостороннюю систему с опорой на основанный на правилах международный порядок, которая способствует результативным усилиям по решению глобальных проблем в киберпространстве. Хорошим примером таких усилий является наше участие в различных межправительственных инициативах и инициативах с участием многих заинтересованных сторон, а также поддержка, которую она оказывает этим инициативам. Венгрия подтверждает применимость действующих норм международного права к поведению государств в киберпространстве, которая была признана в утвержденных консенсусом докладах Группы правительственных экспертов за 2010, 2013 и 2015 годы. Вместе с тем невыполнение государственными и негосударственными субъектами своих обязательств по международному праву по-прежнему представляет собой серьезную угрозу международному миру и безопасности и нашему национальному суверенитету как в материальном мире, так и в киберпространстве. Исходя из этого, мы должны быть в состоянии сдерживать и предотвращать как обычные, так и нетрадиционные виды атак.

Содействие осуществлению Повестки дня в области разоружения

Венгрия разделяет озабоченность, выраженную Генеральным секретарем в связи с ростом масштабов злонамеренного использования ИКТ, и потому поддерживает усилия по созданию мирной ИКТ-среды, которое является одной из приоритетных задач, определенных в Повестке дня в области разоружения, провозглашенной Генеральным секретарем в мае 2018 года. В знак признания наших активных усилий Управление Организации Объединенных Наций по вопросам разоружения включило Венгрию в группу стран, оказывающих поддержку осуществлению действия 31 Повестки дня, которое заключается в содействии обеспечению подотчетности и соблюдению новых стандартов в киберпространстве.

Венгрия поддерживает оказание Генеральным секретарем добрых услуг для сдерживания киберинцидентов, введение в действие добровольных норм поведения в киберпространстве, а также дальнейшее сотрудничество, призванное ликвидировать разрыв между государствами-членами в плане осведомленности о кибертехнологиях.

Кибербезопасность как аспект национальной безопасности

В апреле 2020 года правительство Венгрии приняло новую Стратегию национальной безопасности (прилагается к постановлению правительства № 1163/2020 (IV. 21.)), в соответствии с которой существующая Стратегия национальной кибербезопасности должна быть подвергнута пересмотру. В новой Стратегии национальной безопасности содержится обзор изменений в структуре угроз безопасности за период начиная с 2012 года. Одна из главных целей этого обзора заключается в выявлении, анализе и урегулировании проблем в области безопасности, обусловленных стремительным развитием информационно-коммуникационных технологий.

Ожидается, что количество и изощренность кибератак продолжат расти. Исходя из этого, правительство Венгрии, сотрудничая с другими заинтересованными сторонами, намерено сделать все возможное для укрепления своего

потенциала в целях защиты от кибератак, направленных против критической информационной инфраструктуры страны, а также в целях дальнейшего повышения осведомленности общественности о правилах личной безопасности в киберпространстве.

Одной из первоочередных задач является решение проблем, вызванных распространением искаженной и заведомо ложной информации как в Интернете, так и за его пределами, — особенно сейчас, когда мы продолжаем борьбу с пандемией коронавирусной инфекции (COVID-19). На фоне чрезвычайной ситуации в стране распространение ложной информации может быть особенно опасным.

Укрепление наступательного и оборонительного киберпотенциала должно соответствовать обязательствам государства по международному праву. В противном случае использование наступательных возможностей ИКТ может стать одной из причин милитаризации цифрового пространства.

С нашей точки зрения, потенциал в области кибертехнологий, способный угрожать национальной безопасности и стабильности, рассматривается как оружие, применение которого на определенном уровне уже может рассматриваться как вооруженное нападение, на которое государства также могут отреагировать военными действиями в порядке самообороны. С учетом проблем, связанных с присвоением ответственности в ИКТ-среде, государственные органы при возникновении инцидента в сфере ИКТ должны действовать с должной осмотрительностью и принимать во внимание всю относящуюся к нему информацию, включая более общий контекст события, а также характер и масштабы последствий.

Международное сотрудничество и другие многосторонние инициативы

В качестве члена Европейского союза Венгрия активно участвует в разработке его собственного инструментария кибердипломатии, который позволит Европейскому союзу координировать свои усилия по борьбе со злонамеренными действиями в киберпространстве, которые направлены против его учреждений и государств-членов и источник которых находится за пределами Европейского союза. Подчеркивая важность международного сотрудничества, мы выступаем за расширение диалога с нашими стратегическими партнерами, союзниками и международными организациями.

Ни одна страна или организация не может справиться с современными угрозами безопасности своими силами. Поэтому роль партнерства, и в частности сотрудничества Европейского союза и Организации Североатлантического договора (НАТО), сегодня важнее, чем когда-либо прежде. Нет другого пути, кроме как продолжать и еще более углублять это сотрудничество в предстоящие годы. Противодействие гибридным угрозам (включая угрозы кибербезопасности), безусловно, является одним из основных направлений, на котором обе организации должны сосредоточить свои усилия.

Ожидается, что в ближайшие годы конфликты в киберпространстве еще более обострятся, а разрыв в потенциале между технологически развитыми и развивающимися странами продолжит увеличиваться. В июле 2016 года союзники подтвердили оборонительный мандат НАТО и признали киберпространство одной из сфер операций, в которой НАТО должна вести оборону. В июле 2018 года союзники в очередной раз заявили о готовности НАТО продолжать адаптироваться к изменяющемуся ландшафту киберугроз, на который оказывают влияние как государственные, так и негосударственные субъекты, в том числе финансируемые государствами. Государства — члены НАТО

договорились интегрировать добровольно предоставляемые союзниками национальные киберсредства в операции Организации в рамках строгого политического надзора. Подтверждая свой оборонительный мандат, НАТО заявила о своей решимости использовать весь спектр возможностей, включая киберпотенциал, для сдерживания всего спектра киберугроз, защиты от них и борьбы с ними. НАТО стремится к дальнейшему укреплению партнерских отношений с представителями промышленности и научных кругов всех союзников, чтобы идти в ногу с технологическим прогрессом благодаря инновациям.

Цель обеспечения кибербезопасности для Венгрии не нова. Первое и пока единственное международное соглашение о противодействии киберпреступности, получившее название Конвенции о киберпреступности Совета Европы, которая также известна как Будапештская конвенция, было заключено в 2001 году в Будапеште и с тех пор служит руководством для разработки всеобъемлющего национального законодательства по борьбе с киберпреступностью, а также основой для международного сотрудничества. Конвенция была ратифицирована Законом № LXXIX от 2004 года. Венгрия не только является участником Будапештской конвенции, но и активно содействует присоединению к ней третьих стран.

Вклад Венгрии в деятельность ОБСЕ заключается в том, что ее постоянный представитель начиная с 2017 года выполняет функции Председателя Неофициальной рабочей группы ОБСЕ, созданной в соответствии с решением № 1039 Постоянного совета о разработке мер укрепления доверия в целях снижения рисков возникновения конфликтов в результате использования ИКТ. Венгрия поддерживает усилия по укреплению сотрудничества между процессами Организации Объединенных Наций и другими соответствующими региональными организациями, такими как ОБСЕ. На региональном уровне мы подчеркиваем важность реализации принятого ОБСЕ комплекса мер укрепления доверия. Кроме того, мы выступаем за дальнейшую проработку в рамках Рабочей группы открытого состава вопроса о глобализации региональных мер укрепления доверия. Вместе с тем нам необходимо сосредоточить внимание на том, чтобы одинаково эффективно реализовать каждую из региональных мер укрепления доверия.

Венгрия является одной из немногих стран, в которых имеются специалисты по кибердипломатии. Координатор по вопросам кибертехнологий Министерства иностранных дел и внешнеэкономических связей отвечает за информационно-просветительскую деятельность на международном уровне по вопросам киберпространства в рамках как двусторонних, так и многосторонних отношений, включая инициативы Организации Объединенных Наций, Европейского союза, ОБСЕ и другие многосторонние инициативы в этой области, такие как Глобальный форум по обмену опытом в области компьютерных технологий. Кибердипломатия является для нас относительно новой областью международного сотрудничества, которая может стать полезной для правительства страны в деле борьбы со злонамеренными действиями в киберпространстве.

Венгрия участвует в усилиях по укреплению потенциала в третьих странах. В контексте этих усилий кибербезопасность тоже играет важную роль, являясь неотъемлемой частью политики Венгрии в области международного сотрудничества в целях развития, прежде всего с африканскими странами-партнерами. По линии такого сотрудничества Венгрия предоставляет Уганде помощь в целях развития в области безопасности информационных технологий, чтобы помочь этой стране противостоять вызовам XXI века. Сфера кибербезопасности является одним из основных направлений сотрудничества, фигурирующих в недавно

принятых Венгрией Стратегии сотрудничества с Африкой и Стратегии международного сотрудничества в целях развития на период 2020–2025 годов.

Помимо участия в различных межправительственных переговорах, правительство Венгрии содействует осуществлению таких многосторонних инициатив, как Парижский призыв к доверию и безопасности в киберпространстве, откликаясь на рекомендацию относительно углубления сотрудничества в области разработки норм, правил и принципов поведения государств в киберпространстве. К этим усилиям правительства присоединились десятки частных предприятий Венгрии. Кроме того, Венгрия поддерживает и Крайстчерчский призыв к ликвидации материалов в Интернете, пропагандирующих терроризм и насильственный экстремизм, поскольку эти материалы негативно воздействуют на положение в области прав человека и нашу коллективную безопасность.

Венгрия разделяет мнение о том, что неправительственные субъекты (гражданское общество, научные круги, частный сектор и ИКТ-сообщество) обладают целым рядом технических знаний и/или необходимых ресурсов, с помощью которых они, выполняя свои соответствующие функции и обязанности, могут содействовать созданию безопасного и надежного в долгосрочной перспективе киберпространства. Ведущая роль в поощрении этой координации усилий и сотрудничества принадлежит государствам.

Индонезия

[Подлинный текст на английском языке]
[31 мая 2020 года]

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

В Индонезии насчитывается свыше 170 миллионов пользователей Интернета, что составляет 65 процентов от общей численности населения страны. Информационно-коммуникационные технологии (ИКТ) открывают перед Индонезией возможности, которые имеют жизненно важное значение для достижения целей в области устойчивого развития. С другой стороны, растет и количество проблем, возникающих в киберпространстве. В 2019 году Индонезия столкнулась с более чем 220 млн кибератак, которые препятствовали эффективному использованию киберпространства.

Индонезия активно принимает целый ряд мер в целях максимального использования цифрового потенциала, а также в целях борьбы с киберугрозами путем укрепления правовых и политических аспектов институциональной инфраструктуры, наращивания потенциала и развития международного сотрудничества.

Усилия на национальном уровне

В 2017 году было создано Национальное агентство по кибертехнологиям и криптографии, на которое были возложены функции центрального органа Индонезии по вопросам кибербезопасности. В рамках этого органа создана Национальная группа реагирования на чрезвычайные ситуации в компьютерной сфере для обеспечения быстрого реагирования на инциденты в киберпространстве, направленные против объектов государственной или частной инфраструктуры. Помимо этого, в каждом из центральных и окружных государственных органов, функционирующих в 34 провинциях Индонезии, создана группа

реагирования на инциденты в области компьютерной безопасности для урегулирования инцидентов в киберпространстве и восстановления после них.

В рамках укрепления национальной правовой и политической базы Индонезия приняла Закон об информации и электронных сделках, а также Национальный перспективный план действий в области электронной торговли на период 2017–2019 годов, в котором предусмотрены меры по обеспечению безопасности электронных и цифровых сделок. На основании постановления № 82 Министерства обороны от 2014 года приняты Руководящие принципы обеспечения киберзащиты Индонезии. Кроме того, в национальную систему стандартизации Индонезии были включены международные стандарты безопасности ИКТ, а именно стандарты ИСО/МЭК 27001 и ИСО 15408.

Одним из приоритетных законопроектов, рассмотрение которых запланировано на 2020 год, является проект закона о кибербезопасности Индонезии, и в настоящее время идет соответствующий законодательный процесс. Помимо этого, в стране в настоящее время ведется разработка стратегии национальной кибербезопасности на период 2020–2024 годов, которая охватывает пять основных направлений: наращивание потенциала противодействия киберугрозам, совершенствование правовой базы, укрепление потенциала в области кибертехнологий, содействие росту цифровой экономики и развитие сотрудничества на национальном и международном уровнях.

Кроме того, Индонезия привержена дальнейшему укреплению сотрудничества на национальном уровне, прежде всего с государственными предприятиями, частным сектором и промышленностью, в целях содействия созданию инклюзивной культуры кибербезопасности. В 2018 году правительство Индонезии инициировало Кампанию по повышению грамотности в области кибербезопасности в целях содействия безопасному доступу к Интернету, а также кампанию по борьбе с мошенничеством и травлей в киберпространстве, соблюдению этических норм в социальных сетях, ответственному использованию Интернета и просвещению родителей по вопросам сетевой безопасности детей.

Усилия на международном уровне

В рамках своих многочисленных мероприятий Индонезия продолжает развивать сотрудничество, передовые наработки и потенциал, чтобы содействовать созданию эффективной доктрины кибербезопасности, которая в итоге могла бы быть принята на всех уровнях.

Что касается многостороннего взаимодействия на международном уровне, то Индонезия активно участвует в деятельности Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности, в том числе в качестве координатора Рабочей группы Движения неприсоединившихся стран по разоружению. Кроме того, Индонезия является одним из 25 членов Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

На региональном уровне Индонезия участвует в реализации мер укрепления доверия в рамках Ассоциации государств Юго-Восточной Азии (АСЕАН), в частности, оказывая поддержку в создании контактных центров в секторальных органах АСЕАН, занимающихся вопросами кибертехнологий в рамках таких ее подразделений, как Сообщество по вопросам политического сотрудничества и безопасности и Экономическое сообщество, а также обмениваясь информацией, регулярно взаимодействуя с другими субъектами в вопросах кибербезопасности и поддерживая диалог с государствами-членами. Кроме того, АСЕАН

способствовала укреплению сотрудничества в области кибербезопасности, создав комитет по координации деятельности между сообществами АСЕАН. В ходе Регионального форума АСЕАН обсуждение мер укрепления доверия в контексте кибербезопасности вышло за рамки Ассоциации благодаря присоединившимся к нему другим странам и партнерам.

Помимо этого, Индонезия поддерживает диалог и сотрудничество с различными государствами и партнерами на двустороннем уровне. Индонезия продолжит конструктивно содействовать усилиям по укреплению ответственного поведения государств, а также по созданию открытой, безопасной, стабильной, доступной и мирной ИКТ-среды.

Содержание концепций, упомянутых в докладах Группы правительственных экспертов

Неправомерное использование киберпространства как государственными, так и негосударственными субъектами, включая посредников, создает риски для международного мира и безопасности, а также для стабильности в политической, экономической и социальной сферах на национальном уровне. Кроме того, в настоящее время во всем мире происходит колоссальный сдвиг в сторону использования ИКТ на фоне борьбы с многоплановыми последствиями пандемии коронавирусной инфекции (COVID-19). Злоумышленники, действующие в киберпространстве, могут, в частности, попытаться воспользоваться в своих целях системами ИКТ и возможностями распространения информации в киберпространстве.

Принципиальное значение для укрепления безопасности и стабильности в киберпространстве имеют взаимопонимание, сотрудничество, взаимодействие, меры укрепления доверия, оказание помощи и наращивание потенциала. Все двусторонние, региональные и глобальные усилия в этом отношении необходимо поддерживать и рассматривать как взаимодополняющие, а не конкурирующие друг с другом.

Индонезия поддерживает дальнейшее обсуждение и реализацию не имеющих обязательной силы норм в соответствии с докладом Группы правительственных экспертов за 2015 год. Индонезия подтверждает чрезвычайно важную роль Организации Объединенных Наций и региональных организаций в содействии обсуждению и реализации 11 норм, мер укрепления доверия и потенциала в области кибербезопасности, особенно в интересах сокращения и устранения цифрового разрыва между странами.

Индонезия считает, что добровольные и необязывающие нормы служат важной основой ответственного поведения государств. Пробелы, связанные с неурегулированными вопросами киберпространства, необходимо ликвидировать, поэтому Индонезия приветствует дальнейшее развитие государственной практики и норм обычного права в этом отношении.

Индонезия открыта для обсуждения вопроса о применении действующих норм международного права в киберпространстве, включая возможность применения принципа lex specialis. Индонезия подчеркивает, что киберпространство должно использоваться в соответствии с международно-правовыми принципами, и в первую очередь принципами полного уважения суверенитета, невмешательства, мирного урегулирования споров, а также принципами, лежащими в основе прав человека и Устава Организации Объединенных Наций.

Индонезия поддерживает идею заявления от имени всех государств в рамках Генеральной Ассамблеи о необходимости избегать милитаризации киберпространства, которая подрывает международный мир и безопасность и противоречит правам и обязательствам государств по международному праву.

Индонезия подчеркивает, что следует углублять понимание данной проблемы и активизировать соответствующие усилия, особенно в тех странах и регионах, которые пока не принимают должного участия в обсуждениях вопросов и принятии мер, касающихся кибербезопасности.

Ирландия

[Подлинный текст на английском языке]
[30 мая 2020 года]

Ирландия приветствует предоставленную ей возможность выполнить просьбу Генерального секретаря Организации Объединенных Наций, изложенную в пункте 2 резолюции 74/28 о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности. Кроме того, Ирландия поддерживает позицию, изложенную в материале, представленном Европейским союзом. Информационно-коммуникационные технологии (ИКТ) приносят пользу обществу и государствам, поскольку служат подспорьем в таких областях, как коммуникации, образование, инновации и экономическая деятельность, и способствуют процветанию. Вместе с тем в сегодняшнем все более взаимосвязанном мире злоупотребление этими мощными технологиями также может иметь и весьма негативные последствия, и растущие масштабы злонамеренной деятельности в киберпространстве, в том числе во время нынешней пандемии, вызывают серьезную озабоченность Ирландии. Эта деятельность оказывает негативное влияние на жизнь граждан и подрывает их доверие к институтам. Последствия этой деятельности ощущаются и на уровне общества и государств, где они могут стать причиной возникновения или обострения конфликта. Организация Объединенных Наций остается главным форумом для решения проблем, связанных с неправомерным использованием ИКТ и злонамеренной деятельностью в киберпространстве и негативно сказывающихся на реализации всех трех основных компонентов повестки дня Организации, которыми являются мир и безопасность, права человека и устойчивое развитие. Как страна, уделяющая большое внимание сектору ИКТ и твердо приверженная принципам Организации Объединенных Наций, Ирландия продолжит содействовать Организации в пропаганде и поощрении ответственного поведения государств в киберпространстве. Ирландия также продолжит активно сотрудничать с партнерами в Организации Объединенных Наций и на международном уровне в целях содействия созданию открытого, свободного, безопасного и надежного киберпространства, поощрения свободы выражения мнений, ассоциаций и собраний в режиме онлайн, уменьшения опасности возникновения конфликтов и укрепления мира, а также для обеспечения того, чтобы социальные и экономические блага киберпространства были доступны всем, что, в частности, согласуется с целями в области устойчивого развития. Мы считаем, что добиться устойчивого прогресса в решении стоящих перед нами проблем возможно только при многостороннем и всеохватном участии заинтересованных сторон, которое мы стремимся обеспечивать на национальном уровне в рамках таких инициатив, как Кибертехнологический кластер Ирландии, который был создан в 2019 году при финансовой поддержке правительства и в рамках которого целый ряд заинтересованных представителей промышленности, научных кругов и государственной власти объединился для обсуждения и поощрения сотрудничества, повышения осведомленности о возможностях образования и карьерного

роста, имеющихся в киберпространстве, а также для содействия развитию инноваций в секторе кибербезопасности Ирландии. Эти же цели мы преследуем и на международном уровне и в этой связи с удовлетворением отмечаем инициативы Организации Объединенных Наций и других форумов, направленные на расширение сотрудничества и диалога, в том числе в рамках Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Кроме того, Ирландия поддерживает деятельность Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности.

В основе подхода Ирландии к решению проблем в области кибертехнологий по-прежнему лежит ее убежденность в применимости и принципиальной важности международного права, включая Устав Организации Объединенных Наций, международное гуманитарное право и международное право прав человека. Помимо этого, Ирландия с удовлетворением отмечает достигнутый Генеральной Ассамблеей в 2015 году консенсус в отношении того, что все государства в своей практике использования ИКТ должны руководствоваться докладом Группы правительственных экспертов за 2015 год, содержащим 11 добровольных и необязывающих норм ответственного поведения государств. Мы считаем, что эти нормы в сочетании с нормами международного права, будучи дополнены мерами по формированию потенциала, необходимого для противодействия киберугрозам и расширения доступа к ИКТ, а также мерами укрепления доверия, направленными на снижение риска вооруженных конфликтов, представляют собой прочную основу для содействия более корректному поведению государств в киберпространстве. Кроме того, инициативы по наращиванию потенциала в области ИКТ могут способствовать преодолению сохраняющегося в мире цифрового разрыва, меняя жизнь людей и общин и содействуя процветанию, положительно влияя на ход достижения целей устойчивого развития и ускоряя его, в частности в том что касается гендерных аспектов.

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

Стратегия национальной кибербезопасности Ирландии на период 2019–2024 годов

Поскольку в киберпространстве все взаимосвязано, все государства должны приложить усилия к формированию потенциала противодействия киберугрозам как на национальном, так и на глобальном уровне. В Стратегии национальной кибербезопасности Ирландии на период 2019–2024 годов изложены основные задачи и необходимые действия в этой области[8]. Стратегия согласуется с задачей Организации Объединенных Наций по поощрению ответственного поведения государств в киберпространстве и поддержанию международного мира и безопасности, поскольку преследует цель защитить Ирландию, ее народ и критическую инфраструктуру от угроз в области кибербезопасности. Кроме того, эта стратегия подкрепляет усилия, прилагаемые Ирландией на международном уровне для содействия созданию свободного, открытого, мирного и безопасного киберпространства. За осуществление политики Ирландии в области кибербезопасности отвечает Национальный центр по вопросам кибербезопасности, который вносит свой вклад в реализацию повестки дня Организации Объединенных Наций в области кибертехнологий, содействуя проведению диалога по вопросам киберпространства и сотрудничая с учреждениями-

[8] URL: https://www.dccae.gov.ie/documents/National_Cyber_Security_Strategy.pdf.

партнерами и другими заинтересованными сторонами на международном уровне, и тем самым способствует укреплению доверия и безопасности в киберпространстве. Основные цели, сформулированные в Стратегии кибербезопасности Ирландии, заключаются в следующем:

- продолжать расширять возможности Ирландии по выявлению инцидентов, связанных с кибербезопасностью, реагированию на них и управлению ими;
- обеспечивать выявление и защиту объектов критической национальной инфраструктуры, укрепляя их потенциал противодействия кибератакам;
- укрепить потенциал противодействия и безопасность информационных технологий в государственном секторе в целях более эффективной защиты важных услуг, оказываемых гражданам, и их личных данных;
- инвестировать в образовательные инициативы для подготовки высококвалифицированных кадров в области информационных технологий и кибербезопасности;
- повышать осведомленность предприятий об ответственности за обеспечение безопасности своих сетей, устройств и данных и стимулировать научные исследования и разработки в области кибербезопасности в Ирландии, в том числе путем поощрения инвестиций в новые технологии;
- продолжать взаимодействовать с международными партнерами и международными организациями для обеспечения того, чтобы киберпространство оставалось открытым, безопасным, единым, свободным и продолжало служить катализатором экономического и социального развития, а также неуклонного наращивания потенциала;
- повысить общий уровень навыков и осведомленности частных лиц об основных правилах личной безопасности в киберпространстве и оказать им в этом поддержку, предоставив соответствующую информацию и возможности для обучения.

Правительственный информационный документ по вопросам оборонной политики

В Правительственном информационном документе по вопросам оборонной политики Ирландии (опубликован в 2015 году[9], обновлен в 2019 году[10]) отмечается опасность, которую представляет злонамеренная деятельность с использованием кибертехнологий как на территории страны, так и за рубежом, в частности, для объектов критической инфраструктуры и работы основных служб, а также указывается, что злонамеренное использование кибертехнологий может быть направлено на то, чтобы подорвать основные ценности, такие как человеческое достоинство, свобода и демократия. Данный правительственный документ и Стратегия национальной кибербезопасности продолжают служить основой для деятельности Ирландии в области ИКТ и кибертехнологий.

Двусторонние, региональные и многосторонние подходы

Взаимодействуя с другими государствами на двустороннем уровне, а также в рамках региональных и многосторонних форумов, Ирландия продолжает содействовать диалогу по вопросам ИКТ и кибертехнологий.

[9] URL: https://assets.gov.ie/21963/f1e7723dd1764a4281692f3f7cb96966.pdf.
[10] URL: https://www.gov.ie/en/publication/a519cf-white-paper-on-defence-update-2019/.

Ирландия с удовлетворением отмечает деятельность Организации по безопасности и сотрудничеству в Европе (ОБСЕ) и других региональных организаций во всем мире, направленную на содействие реализации мер укрепления доверия.

Ирландия поддерживает государственные и негосударственные инициативы, способствующие поддержанию доверия, безопасности и мира в киберпространстве, включая Парижский призыв к доверию и безопасности в киберпространстве. Кроме того, Ирландия поддерживает Крайстчерчский призыв к ликвидации материалов в Интернете, пропагандирующих терроризм и насильственный экстремизм. Ирландия является членом Коалиции за свободу в Интернете, в состав которой входит 31 государство; совместными усилиями они содействуют обеспечению свободы в Интернете.

Кроме того, Ирландия представила письмо о намерении, содержащее просьбу о включении в состав Центра передового опыта по совместной кибербезопасности в Таллинне, с тем чтобы совместно с партнерами-единомышленниками внести свой вклад в решение проблем кибербезопасности. К работе этого центра Ирландия намерена присоединиться на правах активного участника, поскольку не является членом НАТО.

Содействие международному сотрудничеству в рамках Европейского союза

Ирландия продолжает полноценно и активно участвовать в деятельности Европейского союза в области кибертехнологий и тесно сотрудничает со своими партнерами по Европейскому союзу, в том числе по линии инициатив в области кибердипломатии и применения инструментария кибердипломатии Европейского союза, стремясь к созданию открытого для всего мира, свободного, стабильного и безопасного киберпространства, которое способствует предотвращению конфликтов. Укрепляя свой потенциал противодействия киберугрозам, Ирландия также участвует в осуществлении ряда инициатив Европейского оборонного агентства.

Содействие международному сотрудничеству в рамках Организации Объединенных Наций

Что касается усилий в рамках Организации Объединенных Наций, то Ирландия поддерживает работу Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (см. также ниже) и активно участвует в деятельности Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Кроме того, 22 мая 2020 года постоянный представитель Ирландии в Организации Объединенных Наций выступила на заседании Совета Безопасности Организации Объединенных Наций по формуле Аррии по вопросам киберстабильности, предотвращения конфликтов и укрепления потенциала, подчеркнув готовность Ирландии сотрудничать с Организацией Объединенных Наций в этой области по широкому кругу направлений, в частности, используя ИКТ и киберпространство для достижения целей в области устойчивого развития и прежде всего цели обеспечения гендерного равенства.

Содержание концепций, упомянутых в докладах Группы правительственных экспертов

Общие принципы

Ирландия выступает за многосторонний подход к поощрению глобальной кибербезопасности без предпочтения каким-либо конкретным технологиям и с опорой международный порядок, основанный на правилах. Ирландия считает, что участие и вклад заинтересованных сторон (включая гражданское общество, научные круги, представителей технологического сектора и промышленности) способствовали более содержательным дискуссиям в ходе недавних совещаний Рабочей группы открытого состава. Эти заинтересованные стороны будут играть все более важную роль в консультировании государств по вопросам дальнейшего развития сферы ИКТ и в непосредственном поддержании безопасности и стабильности киберпространства. Ирландия считает, что расширение участия заинтересованных сторон в предстоящих совещаниях и других дискуссиях по вопросам кибертехнологий является ценным и необходимым и должно получить официальное оформление.

Существующие и новые угрозы

В Стратегии национальной кибербезопасности Ирландии признается растущее положительное влияние ИКТ на экономическое и социальное развитие, но при этом подчеркивается рост киберпреступности, случаев хищения интеллектуальной собственности и распространения дезинформации, а также использования государствами наступательного киберпотенциала. Пандемия коронавирусной инфекции (COVID-19) показала, насколько сильно нам необходимы ИКТ для обеспечения гибкости и безопасности в работе и общении и поддержания экономической деятельности. Вместе с тем пандемия также позволила обратить внимание на деятельность злоумышленников, которые пользуются уязвимостью как техники, так и человека, для совершения киберпреступлений или распространения дезинформации, которая вызывает замешательство, недоверие и раскол в обществе. Ирландия с особой озабоченностью отмечает недавние кибератаки на службы здравоохранения, а также медицинские и смежные учреждения. Подобные нападения на медицинские и другие жизненно важные службы ставят под угрозу жизнь людей. Ирландия вместе со своими партнерами по Европейскому союзу осудила эти нападения и призвала все государства проявлять должную осмотрительность и, в соответствии с международным правом и утвержденными консенсусом докладами Группы правительственных экспертов за 2010, 2013 и 2015 годы, принимать надлежащие меры в отношении субъектов, осуществляющих такую деятельность с территории этих государств.

Международное право

Ирландия твердо убеждена в том, что нормы международного права, включая положения Устава Организации Объединенных Наций, нормы международного гуманитарного права и международного права прав человека, применимы к киберпространству и имеют для него принципиальное значение. Права человека и основные свободы должны соблюдаться как в Интернете, так и за его пределами. Приняв во внимание существующие международно-правовые рамки, Ирландия изложила свои оговорки, в том числе на недавних совещаниях Рабочей группы открытого состава, в отношении призывов к разработке нового правового документа. Вместе с тем Ирландия с удовлетворением отмечает продолжающийся диалог, призванный содействовать более глубокому общему пониманию проблемы применения действующих норм международного права к использованию ИКТ государствами.

Нормы, правила и принципы ответственного поведения государств

Ирландия поддерживает добровольные и необязывающие нормы, правила и принципы ответственного поведения государств, содержащиеся в докладе Группы правительственных экспертов от 2015 года, и приветствует достигнутую консенсусом договоренность Генеральной Ассамблеи о том, что всем государствам следует руководствоваться этим докладом в своей практике использования ИКТ. Эти нормы способствуют обеспечению стабильности и безопасности в глобальной ИКТ-среде и могут стать вкладом в поддержание международного мира. Указанные нормы, правила и принципы, в том числе касающиеся формирования устойчивого потенциала, отражены в Стратегии национальной кибербезопасности Ирландии и политике Ирландии. Ирландия обратилась к Организации Объединенных Наций с призывом продолжить разработку руководящих указаний в отношении того, каким образом эти существующие нормы, утвержденные на основе консенсуса всеми государствами-членами, могут быть введены в действие и применяться на практике.

Меры укрепления доверия

В ходе двусторонних, региональных и многосторонних совещаний и форумов Ирландия активно участвует в обсуждении вопросов ИКТ и кибербезопасности, в том числе в контексте глобального мира и безопасности, устойчивого развития и прав человека, и поощряет проведение соответствующих дискуссий. Ирландия отдает должное масштабной работе региональных организаций, проделанной в интересах укрепления доверия, а также соответствующим инициативам государственных и негосударственных субъектов, включая Парижский призыв, и в целом поддерживает предложения о создании в целях поддержки будущих инициатив механизмов для обмена передовым опытом реализации мер укрепления доверия.

Меры по наращиванию потенциала

В Стратегии национальной кибербезопасности Ирландии содержится обязательство продолжать осуществление эффективных в долгосрочной перспективе мер по укреплению потенциала. Кроме того, Ирландия высоко оценивает многосторонний и основанный на широком участии подход к укреплению потенциала всех государств по борьбе со злонамеренной деятельностью в киберпространстве, уменьшению факторов уязвимости, защите критической инфраструктуры и распространению всех преимуществ доступа к ИКТ на все государства. Помимо этого, Ирландия считает крайне важным, чтобы все государства и основные заинтересованные стороны имели возможность участвовать в дискуссиях по вопросам кибертехнологий на международном уровне. В этой связи Ирландия с готовностью выступила одним из организаторов состоявшегося 2–4 декабря 2019 года неофициального межсессионного совещания Рабочей группы открытого состава, в котором приняли участие как государства, так и заинтересованные представители неправительственных организаций и гражданского общества, технические эксперты, представители научного и академического сообщества, а также частного сектора. Кроме того, Ирландия решительно поддерживает усилия по решению проблемы неравного доступа мужчин и женщин к цифровым технологиям. Ирландия будет приветствовать более тесную увязку предстоящих обсуждений и инициатив Организации Объединенных Наций по наращиванию потенциала с целями в области устойчивого развития и повесткой дня по вопросу о женщинах и мире и безопасности.

Италия

[Подлинный текст на английском языке]
[29 мая 2020 года]

Введение

Италия присоединяется к взглядам, выраженным Европейским союзом в его материале, представленном для включения в настоящий доклад, и хотела бы сообщить Генеральному секретарю следующую информацию о деятельности на национальном уровне.

Для целей настоящего доклада Италия не будет оперировать понятием «информационная безопасность», которое не используется в итальянской правовой системе. В ней приняты другие понятия, такие как «кибербезопасность» или «безопасность сетей и информационных систем», и потому в данном случае их употребление более предпочтительно. Свобода выражения мнений — как в Интернете, так и за его пределами — признана основным законом Италии и статьей 19 Международного пакта о гражданских и политических правах, ратифицированного Италией в 1978 году.

В соответствии с указом премьер-министра Италии от 17 февраля 2017 года, в котором содержатся руководящие принципы защиты национального киберпространства и обеспечения безопасности информационно-коммуникационных технологий, термин «кибербезопасность» относится к защите киберпространства, обеспечиваемой посредством надлежащих мер безопасности физического, логического и процедурного характера с целью предотвращения и урегулирования событий, будь то умышленно вызванных или случайных, связанных с неправомерным получением и передачей данных, их изменением или незаконным уничтожением или ненадлежащим управлением сетями и информационными системами или их компонентами, нанесением им ущерба, их уничтожением или препятствованием их нормальной работе.

В свою очередь, выражение «безопасность сетей и информационных систем» обозначает способность какой-либо сети или информационной системы противодействовать на определенном уровне конфиденциальности любому действию, затрагивающему доступность, аутентичность, целостность или конфиденциальность хранимых, передаваемых или обрабатываемых данных, а также соответствующих услуг, предоставляемых или доступных через эту сеть или информационную систему, как это определено в Законодательном декрете № 65/2018, которым в национальное законодательство включаются положения Директивы Европейского союза о безопасности сетей и информационных систем.

Усилия, прилагаемые на национальном уровне для укрепления кибербезопасности: институциональные и нормативные рамки

В декабре 2013 года Италия приняла Национальные стратегические рамки обеспечения безопасности в киберпространстве, в которых принимаются во внимание растущие и изменяющиеся угрозы, связанные с использованием информационно-коммуникационных технологий (ИКТ) и ставится цель укрепления потенциала Италии в области кибертехнологий и способности противодействия киберугрозам. В разработанных затем национальных планах действий, последний из которых был опубликован в марте 2017 года и утвержден в соответствии с вышеупомянутым указом премьер-министра от 17 февраля 2017 года, определен ряд мер, вопросов и приоритетных задач в контексте осуществления Стратегических рамок.

В указе премьер-министра определена архитектура национальной кибербезопасности и структура управления ею, в соответствии с которой предусматривается создание в Департаменте информации и безопасности Совета по вопросам кибербезопасности, который отвечает за предотвращение кризисных ситуаций в сфере национальной кибербезопасности и подготовку к ним, а также за координацию мер реагирования и восстановительных мероприятий, которые должны осуществляться государственным и частным секторами в соответствии с решениями премьер-министра.

Совет по вопросам кибербезопасности состоит из Секретариата и объединенной комиссии под председательством заместителя генерального директора Департамента информации и безопасности по вопросам кибертехнологий, в состав которой входят представители разведывательного сообщества (Департамента информации и безопасности, Агентства информации и внешней безопасности и Агентства информации и внутренней безопасности), военный советник премьер-министра, представители министерств иностранных дел и международного сотрудничества, внутренних дел, юстиции, обороны, экономики и финансов и экономического развития, Департамента гражданской защиты и Агентства цифрового развития Италии. Представитель Центрального бюро по защите секретной информации Департамента информации и безопасности задействует усилия Совета всякий раз, когда речь идет о событиях, угрожающих безопасности систем, в которых содержатся секретные данные.

В случае возникновения кризисной ситуации в области национальной кибербезопасности в состав Совета могут быть включены также представители Министерства здравоохранения, Министерства инфраструктуры и транспорта и Департамента пожарной охраны. Премьер-министр на основании информации, предоставленной Советом по вопросам кибербезопасности, может объявить о наступлении кризиса в области национальной кибербезопасности, когда какой-либо инцидент в киберпространстве ввиду своих масштабов, интенсивности или характера не может быть урегулирован только одним уполномоченным ведомством и требует совместного и скоординированного подхода, который и обеспечивает Совет по вопросам кибербезопасности.

Вслед за указом премьер-министра были приняты дополнительные законодательные акты, а именно:

- Законодательный декрет № 65/2018, включающий в национальное законодательство положения Директивы Европейского союза о безопасности сетей и информационных систем и наделяющий Департамент информации и безопасности функциями единого контактного центра по вопросам сетей и информационных систем;
- Положения о периметре национальной кибербезопасности (Закон № 133/2019), вступившие в силу в ноябре 2019 года и действующие в отношении государственных и частных организаций страны, выполняющих основные функции или предоставляющих основные услуги, необходимые для осуществления деятельности, считающейся принципиально важной для национальных интересов Италии. Порядок включения государственных и частных организаций в этот периметр определяется степенью их приоритетности для национальной безопасности. Этот закон распространяется на те сети, информационные системы и услуги, которые являются собственностью вышеупомянутых организаций или эксплуатируются ими и могут повлиять на национальную безопасность. В законе предусмотрено следующее:

– необходимость уведомления об инцидентах, с тем чтобы обеспечить оперативное направление информации соответствующим структурам, отвечающим за предотвращение киберинцидентов, подготовку к ним и их урегулирование, а именно Совету по вопросам кибербезопасности и Группе реагирования на инциденты в области компьютерной безопасности, входящим в состав Департамента информации и безопасности;

– меры безопасности, охватывающие организационные вопросы, процессы и процедуры, включая закупки ИКТ;

– проверка технических параметров продуктов и услуг ИКТ, относящихся к определенным категориям и связанных с объектами/структурами, включенными в периметр. В соответствии с этим законом любой субъект, желающий приобрести такие предметы, должен проинформировать об этом Национальный центр оценки и сертификации, который, в свою очередь, может провести предварительную оценку, установить определенные условия и потребовать выполнить тестирование аппаратного или программного обеспечения. В последнем случае в условия соответствующих конкурсных торгов и контрактов должен быть включен пункт, в котором оговаривается возможность приостановления или прекращения выполнения соответствующих обязательств при несоблюдении надлежащих требований или неудовлетворительных результатах тестирования, предписанного Национальным центром оценки и сертификации;

– возложение ответственности за проведение инспекций и применение санкций в отношении государственных и частных субъектов, соответственно, на Президиум Совета министров и министра экономического развития.

В случае возникновения в области национальной безопасности серьезной и непосредственной угрозы, связанной с сетями, информационными системами и услугами, премьер-министр может издать распоряжение о частичном или полном отключении/приостановлении работы одного или нескольких устройств или программных продуктов, установленных в сетях или системах или связанных с предоставлением определенных услуг. Такое решение подлежит предварительному обсуждению в Межведомственном комитете по безопасности Республики и действует в течение периода времени, строго необходимого для устранения или смягчения угрозы, в соответствии с принципом соразмерности.

• Декрет-закон № 22/2019, преобразованный в Закон № 41/2019 (статья 1) и включающий в себя декрет-закон № 21/2012 о «Золотой власти», преобразованный в Закон № 56/2012 «об особых полномочиях в отношении регулирования деятельности коммерческих компаний в секторах обороны и национальной безопасности, а также стратегически значимой деятельности в секторах энергетики, транспорта и связи». Данный декрет-закон предусматривает включение в число стратегически значимых для национальной обороны и безопасности видов деятельности услуги широкополосной электронной связи на основе технологий 5G. Согласно новейшим положениям, о заключении договоров или соглашений о приобретении товаров или услуг, связанных с проектированием, созданием, обслуживанием и организацией работы сетей широкополосной электронной связи на основе технологий 5G, или о приобретении «высокотехнологичных компонентов» для создания или организации работы вышеупомянутых сетей, необходимо уведомлять коллегиальный орган по вопросам исполнения закона о «Золотой власти», созданный при Президиуме Совета министров, всякий раз, когда в этих сделках участвуют субъекты, не имеющие отношения к Европейскому союзу. Смысл этой меры заключается в том, чтобы обеспечить возможность наложить вето или выдвинуть конкретные

требования и условия, которые могут быть изменены или объединены с дополнительными мерами, включая замену соответствующих продуктов и оборудования, если Национальный центр оценки и сертификации обнаружит факторы уязвимости, которые могут поставить под угрозу целостность и безопасность сетей и содержащихся в них данных.

Киберзащита

В опубликованном в 2015 году Правительственном официальном документе по вопросам международной безопасности и обороны признается необходимость защиты и обороны киберпространства, в том числе путем формирования «специализированного оперативного оборонного потенциала ... в целях сохранения прочности политических, экономических и социальных структур». Согласно подготовленному Министерством обороны Документу по долгосрочному планированию на период 2019–2021 годов, необходимо защищать киберпространство от атак, направленных на сетевые и компьютерные службы и объекты критической инфраструктуры. В последние годы в Министерстве обороны был проведен ряд реформ, направленных на усиление его защиты, а также на укрепление его потенциала противодействия негативным внешним факторам и совершенствование его доктрины.

В частности, в 2017 году Министерство обороны Италии учредило Объединенное командование сил кибероперaций — военное командование, ответственное за планирование и проведение кибероперaций в целях обнаружения и нейтрализации угроз и нападений на сети, системы и службы Министерства обороны на территории страны, а также в районах операций за пределами Италии.

Объединенное командование сил кибероперaций было недавно включено в состав нового Командования киберкомпонента вооруженных сил в целях построения единой вертикали подчинения, а также повышения эффективности и координации между всеми соответствующими подразделениями по вопросам кибербезопасности всех вооруженных сил (авиации, армии и флота). Командование киберкомпонента оказывает поддержку Генеральному штабу вооруженных сил Италии и выполняет задачу по проведению оборонительных операций для защиты Министерства обороны Италии и входящих в его структуру органов военного управления от инцидентов и атак в киберпространстве.

Помимо этого, Командование киберкомпонента выполняет следующие функции:

- отвечает за кибербезопасность и киберзащиту сетей Министерства обороны, привлекая для этих целей Группу по реагированию на чрезвычайные ситуации в компьютерной сфере, а также за отслеживание деятельности в киберпространстве, предотвращая и ликвидируя инциденты и чрезвычайные ситуации, затрагивающие оборонный сектор;

- в настоящее время проводит исследование в целях определения для районов военных действий таких правовых рамок, которые будут полностью соответствовать нормам международного права и международного гуманитарного права. В рамках такого исследования ставится цель определить минимальные стандарты и правила применения вооруженной силы для поддержки операций путем выполнения определенных задач в киберпространстве. Потребность в правовой базе возникла, в частности, как следствие проведения в течение последних лет многочисленных национальных и международных мероприятий и учений, в том числе в рамках Организации Североатлантического договора (НАТО).

В рамках Объединенного командования сил кибероперациий была создана киберлаборатория в целях разработки инструментов для анализа факторов уязвимости в сфере кибертехнологий и организации учебных мероприятий.

Среди других мер следует отметить предварительное тестирование в целях создания киберполигона для учебной подготовки по вопросам кибертехнологий в училищах телекоммуникаций вооруженных сил Италии и поддержание сотрудничества с целым рядом итальянских университетов в области кибербезопасности.

Усилия по развитию международного сотрудничества в области кибербезопасности, в том числе в связи с докладами Группы правительственных экспертов

Как говорится в статье 10 Конституции Италии, «правопорядок Италии согласуется с общепризнанными нормами международного права».

Исходя из этого, Италия твердо намерена содействовать применению в киберпространстве действующих норм международного права, включая Устав Организации Объединенных Наций во всей его полноте, что также согласуется с позицией Европейского союза, изложенной им в вышеупомянутом материале; соблюдению правил, норм и принципов ответственного поведения государств, сформулированных действовавшей в 2015 году Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и предыдущими группами; разработке мер укрепления доверия и программ по наращиванию потенциала; регулированию Интернета на основе многостороннего подхода.

Италия поддерживает Парижский призыв к доверию и безопасности в киберпространстве, направленный на принятие совместных мер в целях уменьшения рисков для стабильности киберпространства, а также в целях укрепления доверия и потенциала. Кроме того, Италия принадлежит к числу сторон, подписавших Крайстчерчский призыв к ликвидации материалов в Интернете, пропагандирующих терроризм и насильственный экстремизм.

Содействие деятельности по наращиванию потенциала совместно с третьими странами является частью нашей национальной стратегии кибербезопасности и осуществляется в соответствии с «Выводами Совета о рекомендациях относительно наращивания внешнего киберпотенциала Европейского союза», принятыми Советом по общим вопросам Европейского союза на своем 3629-м заседании, состоявшемся 26 июня 2018 года. Деятельность по наращиванию потенциала совместно с третьими странами сосредоточена главным образом на обмене информацией и передовым опытом, особенно в том, что касается реагирования на инциденты в области компьютерной безопасности, а также на образовании и профессиональной подготовке.

Кроме того, важными элементами стратегии национальной кибербезопасности Италии являются участие в международных форумах и содействие соблюдению норм ответственного поведения государств в киберпространстве. По мере целесообразности обсуждение вопросов международного сотрудничества в области кибербезопасности, в том числе в связи с докладами Группы правительственных экспертов, ведется также в рамках двусторонних и многосторонних диалогов и/или консультаций. Основными многосторонними форумами, в рамках которых Италия активно участвует в укреплении сотрудничества в киберпространстве, являются Организация Объединенных Наций, Европейский союз, НАТО, Организация по безопасности и сотрудничеству в Европе (ОБСЕ), Совет Европы и Группа семи.

Так, 10 и 11 апреля 2017 года Италия принимала у себя совещание министров иностранных дел стран Группы семи, на котором была принята Декларация Группы семи об ответственном поведении государств в киберпространстве. В этой декларации содержится призыв ко всем государствам руководствоваться в своей практике использования ИКТ на совокупную информацию, содержащуюся в докладах групп правительственных экспертов Организации Объединенных Наций по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

В период председательства Италии в ОБСЕ в 2018 году Италия активно поддерживала фактическую реализацию государствами-участниками мер укрепления доверия ОБСЕ в области информационной и телекоммуникационной безопасности, и для этих целей, в частности, организовала дискуссию с рассмотрением конкретных примеров применения этих мер в случае того или иного международного инцидента в киберпространстве, в рамках состоявшейся 27 и 28 сентября 2018 года в Риме Конференции с участием всех государств — членов ОБСЕ по вопросам кибербезопасности/ИКТ 2018 года. В 2019 году Италия в период своего председательства в Азиатской контактной группе ОБСЕ организовала 2 и 3 сентября 2019 года в Токио двадцатую Азиатскую конференцию ОБСЕ на тему «Как достичь всеобъемлющей безопасности в цифровую эпоху: перспективы ОБСЕ и ее азиатских партнеров». Кроме того, Италия содействовала осуществлению ряда проектов ОБСЕ по укреплению потенциала в области кибертехнологий и ИКТ, в том числе проведению 7 и 8 февраля 2019 года в Афинах мероприятия по профессиональной подготовке на субрегиональном уровне по вопросу о роли ИКТ в контексте региональной и международной безопасности.

Италия активно участвует в деятельности Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности и поддерживает работу действующей Группы правительственных экспертов и предыдущих групп. Италия также напоминает, что в резолюции 70/237 Генеральной Ассамблеи подтверждаются выводы, сделанные предыдущими группами правительственных экспертов в их докладах за 2013 и 2015 годы, и призывает государства-члены руководствоваться докладом за 2015 год в своей практике использования информационно-коммуникационных технологий.

Недавно в Министерстве иностранных дел и международного сотрудничества Италии был создан департамент по вопросам кибербезопасности и соответствующей политики в интересах дальнейшего укрепления и поощрения наших дипломатических усилий и международного сотрудничества в этой области.

Япония

[Подлинный текст на английском языке]
[31 мая 2020 года]

Япония рада предоставленной возможности отреагировать на просьбу, содержащуюся в резолюции 74/28 Генеральной Ассамблеи о поощрении ответственного поведения государств в киберпространстве в контексте международной безопасности.

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

Усилия, прилагаемые на национальном уровне для укрепления информационной безопасности

В Японии подготовлена правовая основа для использования данных, включая Основной закон о более эффективном использовании данных государственного и частного секторов и Закон о защите личной информации с внесенными в него поправками. Кроме того, правительство проводит политику формирования общества, которое ориентировано на человека и добивается результатов как в плане экономического развития, так и в решении социальных вопросов благодаря высокой степени интегрированности киберпространства и реального мира. В этих условиях в настоящее время в киберпространстве накапливаются и анализируются огромные объемы данных, получаемых с помощью датчиков и устройств в реальности. Кроме того, в физическом мире мы наблюдаем, как в целом ряде областей с определенной периодичностью появляются и совершенствуются новые продукты и услуги, которые повышают эффективность той или иной деятельности благодаря использованию данных. Киберпространство и физический мир больше нельзя считать независимыми друг от друга сферами, поскольку они так тесно взаимосвязаны, что уже не могут быть отделены друг от друга. Исходя из этого, эти два пространства следует рассматривать как единое, непрерывно развивающееся целое.

Сближение виртуального и реального пространств значительно расширяет возможности для обеспечения благополучия в обществе. В то же время у злоумышленников появляется больше возможностей использовать киберпространство для совершения вредоносных действий. Ожидается, что риск экономических и социальных потерь или ущерба в физическом мире будет возрастать в геометрической прогрессии. В частности, вспышка коронавирусной инфекции (COVID-19), по-видимому, ускоряет тенденцию, в соответствии с которой человечество все больше полагается на информационно-коммуникационные технологии (ИКТ), при этом более явными становятся риски и проблемы, связанные со злонамеренным использованием ИКТ. Все большую озабоченность вызывают сообщения об атаках и злонамеренных действиях в киберпространстве, осуществляемых субъектами, которые пытаются воспользоваться текущим кризисом в своих интересах, и в том числе о вирусах-вымогателях, нарушающих работу медицинских учреждений и государственных структур, а также о распределенных атаках типа «отказ в обслуживании», направленных против медицинских научно-исследовательских учреждений. В этих условиях необходимо обеспечить безопасность киберпространства, которое служит фундаментом общественно-экономического уклада, и в то же время необходимо сделать так, чтобы киберпространство развивалось автономно и непрерывно, что позволит добиться устойчивого прогресса и благосостояния общества.

В последнее время определенные страны, пользуясь своим преимущественным положением, все чаще реагируют на киберугрозы ужесточением государственных мер регулирования и контроля. Однако усиление государственного регулирования и контроля в киберпространстве препятствует его автономному устойчивому развитию. Исходя из этого, необходимо уважать сегодняшнее киберпространство, сформировавшееся на основе автономных инициатив всех заинтересованных сторон, и обеспечивать кибербезопасность совместными усилиями этих сторон. Исходя из этого понимания и памятуя о первоначальных планах на 2020 год и последующий период, Япония приложит все возможные усилия для принятия мер по обеспечению кибербезопасности, уточнив свою

базовую концепцию кибербезопасности, выявив новые проблемы, нуждающиеся в решении, и оперативно приняв соответствующие меры.

Усилия, прилагаемые на национальном уровне для содействия международному сотрудничеству

Поскольку последствия инцидентов в киберпространстве могут легко распространяться за пределы национальных границ, всегда существует вероятность того, что от киберинцидентов в других странах может пострадать и Япония. Япония намерена сотрудничать и взаимодействовать с правительствами и частным сектором во всем мире в целях обеспечения безопасности киберпространства и работать как на благо мира и стабильности международного сообщества, так и на благо своей национальной безопасности. С этой целью правительство нашей страны будет активно участвовать в различных международных дискуссиях и содействовать обмену информацией и выработке общего понимания по вопросам, связанным с кибертехнологиями. Кроме того, правительство намерено делиться опытом с зарубежными странами, налаживать сотрудничество и взаимодействие в конкретных областях и принимать необходимые меры. Помимо этого, правительство будет активно участвовать в международных дискуссиях по проблемам кибербезопасности, которые возникли на фоне вспышки COVID-19.

Что касается обмена опытом и координации политики, то правительство, действуя в рамках двусторонних диалогов и международных конференций по вопросам кибербезопасности, будет содействовать обмену информацией о политике, стратегиях и системах реагирования в области кибербезопасности и применять эти знания при планировании политики Японии в области кибербезопасности. Кроме того, мы будем укреплять сотрудничество и взаимодействие в области политики кибербезопасности со стратегическими партнерами, которые разделяют наши основные принципы кибербезопасности.

Что касается международного сотрудничества в деле реагирования на инциденты, то правительство планирует обмениваться информацией о кибератаках и угрозах и укреплять сотрудничество между группами по реагированию на чрезвычайные ситуации в компьютерной сфере, чтобы обеспечить принятие скоординированных мер реагирования при возникновении инцидентов. Помимо этого, правительство будет работать над укреплением потенциала скоординированного реагирования, организуя для этих целей совместную учебную подготовку и участвуя в международных учениях. Кроме того, при возникновении инцидентов правительство будет принимать надлежащие меры реагирования, опираясь на международное сотрудничество в соответствующей сфере.

С учетом дипломатических аспектов международного сотрудничества в области кибертехнологий мы взяли на себя обязательства в трех основных сферах: обеспечение верховенства права, принятие мер укрепления доверия и наращивание потенциала в киберпространстве.

Содействие обеспечению верховенства права имеет большое значение как для международного мира и стабильности, так и для национальной безопасности Японии. Позиция Японии заключается в том, что действующие нормы международного права, включая положения Устава Организации Объединенных Наций, применимы и к киберпространству, и Япония будет активно содействовать обсуждению вопросов индивидуального и конкретного применения действующих норм международного права и разработки и универсализации норм. Что касается мер по борьбе с киберпреступностью, то Национальное полицейское управление, сотрудничая с другими соответствующими министерствами и ведомствами, будет работать над дальнейшим укреплением международных

партнерских связей, налаживая сотрудничество между странами при проведении расследований и обмен информацией с международными организациями, а также правоохранительными органами и информационными службами безопасности иностранных государств и прибегая к помощи таких механизмов, как Конвенция о киберпреступности, договоры о взаимной правовой помощи и Международная организация уголовной полиции (Интерпол).

Япония будет работать над укреплением доверия между государствами в целях предотвращения кибератак. Ввиду анонимного и секретного характера кибератак существует риск того, что они могут непреднамеренно усилить напряженность в отношениях между государствами. Для предотвращения таких случайных и ненужных конфронтаций важно, чтобы в мирное время были налажены международные каналы связи в рамках подготовки к инцидентам, последствия которых распространяются за пределы национальных границ. Необходимо также повышать транспарентность и укреплять доверие между государствами, активно обмениваясь информацией и поддерживая диалог по вопросам политики в рамках двусторонних и многосторонних консультаций. Кроме того, правительство Японии намерено сотрудничать с другими государствами в целях рассмотрения вопроса о создании механизма, который позволит координировать решение проблем, связанных с киберпространством. В этой связи Япония активно содействует реализации мер укрепления доверия, для чего, в частности, в ходе Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН) она организовала межсессионное совещание по вопросам кибербезопасности, выступив на нем в роли сопредседателя, а также неизменно оказывает помощь в наращивании потенциала, в первую очередь странам Азиатско-Тихоокеанского региона.

Что касается наращивания потенциала, то ввиду усиления взаимозависимости между странами Япония не в состоянии обеспечить мир и стабильность собственными силами. Огромное значение для обеспечения национальной безопасности Японии имеет координация действия на глобальном уровне, направленная на уменьшение и устранение факторов уязвимости в области кибербезопасности. С этой точки зрения содействие наращиванию потенциала в других государствах гарантирует стабильное существование и деятельность как японским гражданам, так и японским компаниям, работающим на территории этих стран и пользующимся их критической инфраструктурой, а также способствует более устойчивому прогрессу в том, что касается использования киберпространства в этих государствах. В то же время меры по наращиванию потенциала напрямую связаны и с обеспечением безопасности всего киберпространства и способствуют улучшению обстановки в области безопасности во всем мире, включая Японию. Кроме того, что касается киберпреступности, то Япония первой из азиатских стран ратифицировала Конвенцию о киберпреступности и всячески содействует ее осуществлению как важной правовой основы для борьбы с киберпреступностью путем оказания помощи странам Азиатского региона в наращивании потенциала.

2. Содержание концепций, упомянутых в докладах Группы правительственных экспертов

По мнению Японии, всем государствам было бы важно и полезно принять во внимание перечисленные ниже концепции, которые были определены Группой правительственных экспертов.

Влияние злонамеренных действий с использованием кибертехнологий на международное сообщество

Для того чтобы обеспечить гибкую интеграцию стремительно развивающихся ИКТ в нашу жизнь и предотвратить ущерб от злонамеренных действий с использованием кибертехнологий, мы должны признать важность прогнозирования известных и потенциальных угроз в киберпространстве и их влияния на международное сообщество.

Соблюдение добровольных и необязывающих норм ответственного поведения государств

Для того чтобы свести к минимуму последствия злонамеренных действий с использованием кибертехнологий и остановить злоумышленников, мы должны помнить о важности утвержденного консенсусом доклада Группы правительственных экспертов, включая упоминаемые в нем добровольные и необязывающие нормы ответственного поведения государств. Взаимодействуя с соответствующими региональными организациями, мы должны углубить наши дискуссии, чтобы обеспечить практическое и эффективное применение этих ценных наработок.

Содействие соблюдению добровольных и необязывающих норм ответственного поведения государств и сотрудничество в целях принятия соответствующих мер укрепления доверия и наращивания потенциала

Для дальнейшего укрепления усилий каждого государства по развитию и поддержанию свободного, справедливого и безопасного киберпространства в контексте международной безопасности нам следует подтвердить, что все государства твердо намерены устранять изъяны в плане безопасности в киберпространстве и предотвращать злонамеренные действия с использованием кибертехнологий, направленные на извлечение выгоды. В этой связи членам Группы следует систематически рекомендовать всем государствам последовательно соблюдать добровольные и необязывающие нормы ответственного поведения государств, включая меры укрепления доверия, и поддерживать сотрудничество, в том числе в рамках работы следующей Группы правительственных экспертов и Рабочей группы открытого состава, в целях наращивания национального потенциала для применения на практике вышеупомянутых добровольных и необязывающих норм и рекомендаций.

Мексика

[Подлинный текст на испанском языке]
[29 мая 2020 года]

Информационные технологии и новые достижения в области телекоммуникаций расширили возможности для устойчивого развития и создания мира, основанного на соблюдении прав, справедливости и инклюзивности. Обеспечение мирного использования этих технологий для общего блага сегодня является обязанностью всего международного сообщества.

Дискуссии в Организации Объединенных Наций по вопросам стабильности в киберпространстве, кибербезопасности и регулирования киберпространства, и в частности доклады, которые были подготовлены Группой правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности в целях содействия ответственному поведению государств в киберпространстве, закладывают основу для

прогресса в деле создания открытого, свободного, стабильного и безопасного киберпространства.

С учетом этих событий правительство Мексики представляет настоящий доклад, будучи убеждено в ценности резолюций, принятых Генеральной Ассамблеей по этому вопросу и в том, что только многосторонний подход позволит в долгосрочной перспективе гарантировать законное и мирное использование киберпространства, наличие потенциала противодействия в цифровой среде, способность информационных технологий содействовать устойчивому развитию и защиту прав человека в киберпространстве.

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

Ниже перечислены созданные правительством Мексики национальные координационные механизмы по вопросам информационной безопасности и органы реагирования.

a) Специальный комитет по информационной безопасности

Этот комитет является межведомственным коллегиальным органом, который отвечает за разработку политики информационной безопасности, применимой к органам национальной безопасности, а также за обеспечение ее надлежащего применения на территории Мексики. В состав Комитета входят представители федеральных структур Мексики, отвечающих за национальную безопасность, общественную безопасность, телекоммуникации, финансовый сектор и внешнюю политику. К числу инициатив, предпринятых этим Комитетом, относятся, в частности, разработка и обновление национальной стратегии кибербезопасности, проведение учений по реагированию на компьютерные инциденты и организация мероприятий по повышению осведомленности в области информационной безопасности.

b) Национальный центр реагирования на инциденты в области кибертехнологий

Этот орган входит в структуру недавно созданной Национальной гвардии Мексики и отвечает за обеспечение целостности стратегической технологической инфраструктуры страны. Национальный центр располагает специализированными подразделениями по предупреждению и расследованию случаев противоправного поведения с использованием компьютерных средств, а также осуществляет мониторинг сетей для выявления преступной деятельности, проводя мероприятия по обеспечению кибербезопасности в целях уменьшения и ослабления рисков киберинцидентов и кибератак. Кроме того, он осуществляет программы по наращиванию научно-технического потенциала в области кибертехнологий.

c) Группа реагирования на инциденты в области безопасности конфиденциальной информации

Эта группа была создана в качестве координационного механизма для обеспечения эффективного реагирования на инциденты в области информационной безопасности в финансовом секторе; в ее работе участвуют генеральная прокуратура, государственные финансовые структуры и профессиональные объединения специалистов из финансового сектора Мексики, а ее цель заключается в обеспечении эффективного реагирования на инциденты, непосредственно затрагивающие финансовый сектор.

На национальном уровне Мексика в последние годы приняла нижеследующие меры по укреплению информационной безопасности.

Правительство Мексики через посредство Министерства общественной безопасности и защиты граждан ежегодно организует Национальную неделю кибербезопасности. Это мероприятие призвано служить площадкой для диалога о методах обеспечения кибербезопасности, способствуя налаживанию партнерства между задействованными в нем секторами в целях поддержания безопасной цифровой среды, устойчивой к негативным воздействиям. Помимо этого, целью данного мероприятия является повышение осведомленности граждан об информационных технологиях и цифровой безопасности в рамках конференций, дискуссионных форумов, учебных занятий, практикумов, вебинаров и развлекательной программы.

С 2018 года правительство Мексики совместно с Организацией американских государств (ОАГ) и компанией «Тренд микро» ежегодно проводит мероприятие под названием «Киберженщины принимают вызов». Цель данного мероприятия заключается в поощрении гендерного равенства в контексте осуществления деятельности, связанной с защитой от угроз кибербезопасности и реагированием на них, а также в формировании и укреплении институционального потенциала в соответствующей области.

В течение 2019 года Министерство связи и транспорта организовывало совещания рабочих групп по кибербезопасности, в которых приняли участие более 5000 человек, пользующихся услугами созданных министерством центров охвата цифровыми технологиями, которые функционируют по всей стране. Основное внимание в ходе этих совещаний уделялось выявлению небезопасного поведения при пользовании услугами телерадиокоммуникации. Данные, полученные в ходе этих совещаний, были использованы при подготовке доклада, озаглавленного «Привычки пользователей по состоянию на 2019 год в контексте кибербезопасности Мексики».

На основе выводов, содержащихся в этом докладе, при поддержке ОАГ и правительства Соединенного Королевства был разработан тренажер-симулятор. Этот симулятор представляет собой инструмент, который позволяет пользователю испытать на себе симулированные киберугрозы в интерактивной среде, после чего оценивается способность пользователя адекватно реагировать на эти угрозы и предлагаются рекомендации, касающиеся оптимальных способов защиты.

Помимо этого, в целях содействия укреплению международного сотрудничества и более ответственному поведению государств в киберпространстве Мексика принимает участие в следующих многосторонних и региональных форумах, механизмах и инициативах:

а) Первый комитет Генеральной Ассамблеи Организации Объединенных Наций

Мексика участвует в деятельности созданной в соответствии с резолюцией 73/27 Генеральной Ассамблеи Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности.

Кроме того, один правительственный эксперт от Мексики участвует в работе учрежденной в соответствии с резолюцией 73/266 Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности.

Мексика стремится обеспечить взаимодополняемость усилий этих двух групп, признавая при этом, что обе они опираются на результаты работы предыдущих групп правительственных экспертов и их доклады, утвержденные Генеральной Ассамблеей на основе консенсуса.

b) Группа друзей по цифровым технологиям

Мексика считает крайне важным разрабатывать и осуществлять на основе сотрудничества меры, связанные с цифровыми технологиями, в особенности такие меры, которые способствуют достижению целей в области устойчивого развития и выполнению связанных с ними задач благодаря эффективному использованию информационных и телекоммуникационных технологий. В соответствии с этой концепцией Мексика, наряду с Сингапуром и Финляндией, с ноября 2019 года выполняет функции сопредседателя Группы друзей по цифровым технологиям, задача которой заключается в содействии инклюзивному диалогу со всеми заинтересованными сторонами в целях рассмотрения связей между цифровыми технологиями и устойчивым развитием, а также в обсуждении возможных форм межсекторального сотрудничества в этой области на международном уровне.

c) Группа высокого уровня по цифровому сотрудничеству

Во исполнение рекомендаций Группы высокого уровня по цифровому сотрудничеству Мексика совместно со Структурой Организации Объединенных Наций по вопросам гендерного равенства и расширения прав и возможностей женщин (Структура «ООН-женщины») провела групповую дискуссию в целях определения конкретных шагов, которые необходимо предпринять для выполнения рекомендаций 1 c) и 1 d), касающихся обеспечения доступности цифровых технологий и выработки соответствующих количественных показателей.

d) Международный союз электросвязи

Мексика участвует в инициативах в области информационной безопасности, координируемых Международным союзом электросвязи и кибербезопасности, включая Глобальную программу кибербезопасности и Глобальный индекс кибербезопасности.

Что касается Глобальной программы кибербезопасности, то Мексика считает ее важной инициативой, которая способствует созданию более безопасной и устойчивой к негативным воздействиям цифровой среды и сама по себе является крайне ценной, поскольку в ее осуществлении задействованы все соответствующие стороны, включая государства, частный сектор, гражданское общество и научные круги.

e) Организация американских государств

Мексика активно участвует в программе кибербезопасности Межамериканского комитета по борьбе с терроризмом ОАГ, созданной в целях содействия разработке политики, наращиванию потенциала, проведению исследований и информационно-просветительской работы по вопросам кибербезопасности в Северной и Южной Америке.

Помимо этого, Национальный центр реагирования на инциденты в области кибертехнологий участвует в работе сети групп реагирования на инциденты в области компьютерной безопасности стран Северной и Южной Америки, функционирующей в рамках программы кибербезопасности Межамериканского комитета по борьбе с терроризмом ОАГ.

Кроме того, Мексика участвует в деятельности Рабочей группы по сотрудничеству и мерам укрепления доверия в киберпространстве Межамериканского комитета по борьбе с терроризмом ОАГ. По итогам работы этой группы, которая была создана в 2018 году, были утверждены меры укрепления доверия, которые заключаются в следующем:

- предоставлять информацию о национальной политике в области кибербезопасности, включая национальные стратегии, правительственные информационные документы, правовые рамки и другие документы, которые то или иное государство-член считает важными в этом контексте;
- уполномочить какую-либо из структур выполнять функции национального контактного центра на политическом уровне для обсуждения последствий киберугроз в Западном полушарии;
- в случае отсутствия в министерствах иностранных дел контактных центров наделить этими функциями соответствующие подразделения в целях поддержки усилий по налаживанию международного сотрудничества и взаимодействия в сфере кибербезопасности и киберпространства;
- развивать и укреплять деятельность по формированию потенциала, организуя такие мероприятия, как семинары, конференции и практикумы, посвященные вопросам кибердипломатии, для государственных должностных лиц и сотрудников частных предприятий;
- поощрять включение вопросов кибербезопасности и киберпространства в программы базовой подготовки и повышения квалификации дипломатов и должностных лиц министерств иностранных дел и других государственных учреждений;
- содействовать сотрудничеству и обмену передовым опытом в области кибердипломатии, кибербезопасности и деятельности в киберпространстве, создавая для этих целей рабочие группы и другие механизмы диалога и заключая межгосударственные соглашения.

f) Глобальный форум по обмену опытом в области компьютерных технологий

В работе этого форума, которая заключается в укреплении потенциала в области кибербезопасности, Мексика участвует с 2015 года. Интерес для Мексики представляют следующие темы: предотвращение кибератак, защита данных, предупреждение киберпреступности (включая детскую порнографию и аналогичные преступления), усилия по созданию электронного правительства и цифровые стратегии, защита критической инфраструктуры, использование ИКТ и Интернета в мирных целях и применимость норм международного права к деятельности в киберпространстве.

g) Форум групп оперативного реагирования и обеспечения безопасности

Национальный центр реагирования на инциденты в области кибертехнологий участвует в работе Форума групп оперативного реагирования и обеспечения безопасности — всемирного форума, в рамках которого объединяются и взаимодействуют группы реагирования на киберинциденты из всех стран мира. Это позволяет создавать и укреплять методы расследования, с помощью которых, сотрудничая с подразделениями полиции других стран по борьбе с киберпреступностью, можно выявить лиц, предположительно ответственных за кибератаки, и определить их местонахождение.

2. Содержание концепций, упомянутых в докладах Группы правительственных экспертов

В соответствии с заявлениями, содержащимися в предыдущих докладах Группы правительственных экспертов, Мексика считает, что международное право применимо к деятельности в киберпространстве. В целях практического осуществления этого принципа правительство Мексики прилагает усилия на национальном уровне, продвигая позицию, в соответствии с которой к нормам, применимым в этой области, относятся положения Устава Организации Объединенных Наций, международные нормы в области прав человека, нормы международного гуманитарного права, некоторые нормы обычного международного права и даже соответствующая судебная практика.

Учитывая содержание предыдущих докладов Группы правительственных экспертов, Мексика признает ту роль, которую могут играть в этой связи региональные организации, и их потенциальный вклад, прежде всего в осуществление мер укрепления доверия. Исходя из этого, правительство Мексики рекомендовало национальным органам рассмотреть вопрос о внедрении мер укрепления доверия, изложенных в докладах Группы правительственных экспертов и получивших дальнейшее развитие в рамках ОАГ.

Мексика придает первостепенное значение концепции укрепления потенциала, вытекающей из докладов Группы правительственных экспертов, поскольку эта концепция касается не только наращивания национального потенциала в области информационной безопасности, но и необходимости использования всех форм международного сотрудничества, которые доказали свою эффективность с точки зрения содействия поддержанию международного мира и безопасности. Наращивание потенциала позволяет государствам и всем другим заинтересованным сторонам лучше подготовиться к борьбе с киберугрозами и способствует выработке общей позиции по определенным вопросам, связанным с кибербезопасностью.

Помимо вышесказанного, в отчетный период правительство Мексики стремилось содействовать синергическому взаимодействию различных групп, форумов, органов и инициатив системы Организации Объединенных Наций, которые занимаются вопросами, связанными с информационными технологиями, телекоммуникациями, кибербезопасностью, регулированием киберпространства, цифровым сотрудничеством и технологическими преобразованиями, что делалось в интересах достижения большей согласованности, недопущения дублирования усилий и более эффективного использования ресурсов, выделяемых на цели сотрудничества.

Сингапур

[Подлинный текст на английском языке]
[27 апреля 2020 года]

Сингапур твердо привержен идее установления в киберпространстве международного порядка, который будет основываться на правилах и станет необходимым фундаментом для доверительных отношений между государствами-членами, а также будет способствовать экономическому и социальному прогрессу. Чтобы в полной мере воспользоваться преимуществами цифровых технологий, международное сообщество должно создать безопасное, надежное и открытое киберпространство, функционирующее 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 таких законов, правил и норм в рамках Организации Объединенных Наций — единственного универсального, инклюзивного и многостороннего форума, где все государства имеют право голоса.

Сингапур участвует в деятельности как Группы правительственных экспертов по поощрению ответственного поведения государств в киберпространстве в контексте международной безопасности, так и Рабочей группы открытого состава по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности. Сингапур вновь заявляет, что рассматривает эти две площадки как взаимодополняющие и будет и впредь конструктивно содействовать работе обеих групп. Для того чтобы деятельность обеих групп увенчалась успехом, она должна осуществляться в духе конструктивного сотрудничества, консенсуса, взаимного уважения и доверия. В качестве сопредседателя Группы друзей по электронному управлению и кибербезопасности Сингапур совместно с Эстонией намерен прилагать активные усилия, чтобы привлечь все страны к оказанию поддержки обеим группам в их работе. Сингапур считает, что неофициальное межсессионное консультативное совещание Рабочей группы открытого состава под председательством руководителя Агентства кибербезопасности Сингапура Дэвида Ко было полезным с точки зрения содействия интерактивному обмену мнениями между государствами-членами, частным сектором, гражданским обществом, научными кругами и техническим сообществом по целому ряду существенных вопросов.

Сингапур считает, что государствам необходимо содействовать повышению осведомленности о существующих добровольных необязывающих нормах ответственного поведения государств и поддерживать их внедрение. Сингапур поддерживает дальнейшее совершенствование таких норм по мере необходимости. Так, в частности, критическую информационную инфраструктуру наднационального уровня можно было бы считать особой категорией критической инфраструктуры, совместная ответственность по защите которой лежит на всех государствах-членах и может быть включена в существующий свод норм[11].

Важную роль могут играть региональные организации. Ассоциация государств Юго-Восточной Азии (АСЕАН) подтвердила необходимость установления международного порядка в киберпространстве, 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 в целом поддержать 11 норм, которые содержатся в докладе Группы правительственных экспертов за 2015 год, а также сосредоточить внимание на укреплении потенциала по соблюдению этих норм на региональном уровне. В октябре 2019 года на четвертой Конференции на уровне министров стран — членов АСЕАН по вопросам кибербезопасности было принято решение о создании комитета рабочего уровня 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 чрезвычайные ситуации в компьютерной сфере, защита критической информационной инфраструктуры и оказание взаимной помощи в вопросах кибербезопасности.

[11] К критической информационной инфраструктуре наднационального уровня относятся объекты, которые принадлежат частным компаниям и функционируют на трансграничной основе, при этом не подпадая под юрисдикцию какого-либо одного государства.

Для того чтобы государства имели возможность эффективно соблюдать правила и нормы ответственного поведения, крайне важно работать над укреплением потенциала. В рамках этих усилий Сингапур в 2016 году учредил Программу укрепления киберпотенциала АСЕАН, на осуществление которой выделено 10 млн сингапурских долларов, в целях содействия наращиванию в странах АСЕАН необходимого потенциала для выработки политики и стратегий, касающихся киберпространства, и решения соответствующих технических вопросов. На сегодняшний день подготовку в рамках этой программы прошли 170 должностных лиц из государств — членов АСЕАН. Стремясь расширить масштабы деятельности, осуществляемой в рамках программы укрепления киберпотенциала АСЕАН, Сингапур в октябре 2019 году открыл Центр передового опыта АСЕАН — Сингапур в области кибербезопасности, бюджет которого составляет 30 млн сингапурских долларов, в целях дальнейшего содействия разработке политики в области кибербезопасности и соответствующих стратегий и наращиванию технического и оперативного потенциала в странах АСЕАН, а также в целях более тесного взаимодействия с международными партнерами.

Кроме того, в рамках совместной программы Организации Объединенных Наций и Сингапура в области кибертехнологий Сингапур выступил одним из организаторов практикума, целью которого было повышение осведомленности государств — членов АСЕАН о нормах поведения и планировании политики в связи с возможными ситуациями в киберпространстве. Помимо этого, совместно с Управлением по вопросам разоружения Сингапур разработал программный учебный онлайн-курс, доступ к которому предоставлен всем государствам — членам Организации Объединенных Наций. Цель курса — способствовать более глубокому пониманию использования информационно-коммуникационных технологий (ИКТ) и их последствий для международной безопасности. Сингапур также обеспечил разработку нескольких учебных курсов по вопросам кибербезопасности, предлагаемых в рамках Сингапурской программы сотрудничества. Мы по-прежнему готовы делиться своим опытом и знаниями с государствами — членами Организации Объединенных Наций, в особенности с малыми и развивающимися странами.

На национальном уровне Сингапур продолжает укреплять кибербезопасность своих систем и сетей по трем направлениям: создание устойчивой к внешним воздействиям инфраструктуры, формирование более безопасного киберпространства и развитие динамичной экосистемы кибербезопасности, — и предпринимает для этого следующие шаги:

а) *создание инфраструктуры, устойчивой к внешним воздействиям.* В рамках непрерывных усилий Сингапура по повышению безопасности и потенциала противодействия секторов его критической информационной инфраструктуры, отвечающих за оказание основных услуг, Агентство кибербезопасности Сингапура разработало Генеральный план обеспечения кибербезопасности в сфере производственных технологий. Генеральный план был разработан с целью усовершенствовать межсекторальные меры, направленные на смягчение киберугроз при эксплуатации производственных технологий, а также на укрепление партнерских отношений с промышленными предприятиями и другими заинтересованными сторонами. В Генеральном плане обеспечения кибербезопасности в сфере производственных технологий изложены основные инициативы, охватывающие людские ресурсы, процессы и технологии и направленные на укрепление потенциала владельцев критической информационной инфраструктуры и организаций, использующих производственные технологические системы;

b) *формирование более безопасного киберпространства.* В рамках усилий по повышению безопасности своего киберпространства и уровня кибергигиены Сингапур в 2020 году планирует ввести систему маркировки уровня кибербезопасности для сетевых интеллектуальных устройств. На начальном этапе система маркировки уровня кибербезопасности будет внедряться в добровольном порядке, чтобы предоставить рынку и разработчикам достаточно времени для осознания того, чем данная система может быть для них полезна. На соответствующих ярлыках кибербезопасности будет указываться уровень безопасности, который гарантируется при использовании того или иного устройства. Благодаря информации, указанной на ярлыке кибербезопасности, потребители могут выбирать ту продукцию, которая имеет наиболее высокий рейтинг с точки зрения безопасности. Система маркировки уровня кибербезопасности призвана мотивировать производителей разрабатывать и выпускать продукцию, обеспечивающую более высокий уровень кибербезопасности, соответствующий общепризнанным стандартам;

c) *развитие динамичной экосистемы кибербезопасности.* Сингапур признает, что укрепление кибербезопасности предполагает создание экосистемы кибербезопасности и поощрение инноваций в этой отрасли. Растет также потребность в формировании резерва из выдающихся специалистов, которые могли бы взять на себя руководство вопросами кибербезопасности в организациях. С момента своего создания в 2015 году Агентство кибербезопасности сотрудничает с государственными учреждениями, профессиональными объединениями, партнерами в сфере промышленности и высшими учебными заведениями Сингапура в целях увеличения численности и повышения квалификации кадров, занимающихся вопросами кибербезопасности. Агентство кибербезопасности возглавляет усилия по реализации национальной инициативы «Перспективные кадры Сингапура в сфере кибербезопасности», направленной на привлечение и поддержку талантливых энтузиастов, интересующихся вопросами кибербезопасности, начиная с раннего возраста, а также на оказание помощи специалистам по кибербезопасности в совершенствовании их навыков. Планируется, что инициативой «Перспективные кадры Сингапура в сфере кибербезопасности» будет охвачено как минимум 20 000 человек в течение трех лет.

Турция

[Подлинный текст на английском языке]
[22 мая 2020 года]

Усилия, предпринимаемые Турцией на национальном уровне в целях укрепления информационной безопасности и развития международного сотрудничества

Информационно-коммуникационные технологии (ИКТ) прочно вошли в социально-экономическую жизнь. 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 ИКТ играют важную роль в достижении устойчивого роста и развития. Однако, чем больше мы используем технологии, тем сильнее мы от них зависим и тем больше оказываемся подверженными рискам, которые сопряжены с их использованием. Отдельные лица, компании, критически важные объекты инфраструктуры и государства — все они сталкиваются с серьезными проблемами, вызванными киберугрозами.

Турция уделяет особое внимание принятию мер, необходимых для укрепления национальной кибербезопасности. Министерство транспорта и инфраструктуры — ведомство, отвечающее в Турции за разработку политики, стратегий и планов действий в области национальной кибербезопасности. В этом контексте были разработаны национальная стратегия и план действий в области кибербезопасности с привлечением всех соответствующих заинтересованных сторон к работе исследовательских комиссий, которую координировало Министерство транспорта и инфраструктуры. Были опубликованы и реализованы национальная стратегия и план действий в области кибербезопасности на 2013–2014 годы и национальная стратегия и план действий в области кибербезопасности на 2016–2019 годы. Турция разрабатывает свои следующие национальную стратегию и план действий в области кибербезопасности, которые, как планируется, охватят период 2020–2023 годов и будут опубликованы в ближайшее время.

Следующие национальная стратегия и план действий Турции в области кибербезопасности преследуют, главным образом, следующие стратегические цели:

- Защита важнейших объектов инфраструктуры и повышение их жизнеустойчивости;
- Укрепление потенциала;
- Безопасность новых технологий (Интернет вещей, сеть 5G, облачные технологи и т.д.);
- Борьба с киберпреступностью;
- Развитие и поддержка национальных технологий;
- Органическая сеть кибербезопасности;
- Развитие международного сотрудничества.

Более того, с 2013 года в Турции работу по противодействию инцидентам в киберпространстве координирует Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве, входящая в состав Управления информационно-коммуникационных технологий. Помимо выявления киберугроз и реагирования на инциденты в киберпространстве, в том числе до, во время и после инцидентов, вышеуказанная группа отвечает за реализацию превентивных мер в отношении киберугроз и обеспечивает их сдерживание в киберпространстве. В сфере кибербезопасности эта группа обращает основное внимание на следующие вопросы: наращивание потенциала в киберпространстве, технологические меры, сбор разведывательной информации об угрозах и обмен ею, а также защита важнейшей инфраструктуры.

В рамках работы по укреплению национальной кибербезопасности с 2013 года для критически важной инфраструктуры или важнейших секторов (например, энергетика, здравоохранение, банковское дело и финансы, управление водными ресурсами, электронная связь и важнейшие государственные услуги) были созданы 14 секторальных и 1299 институциональных групп по реагированию на чрезвычайные ситуации в киберпространстве. Все они работают ежедневно и круглосуточно в целях смягчения рисков в киберпространстве и борьбы с киберугрозами, а их работу координирует национальная группа.

Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве организует и поддерживает учебные курсы, летние лагеря и соревнования по кибербезопасности, которые открыты для нескольких сообществ. Кроме того, она проводит для групп по реагированию на чрезвычайные ситуации в киберпространстве учебные занятия на тему анализа вредоносных

программ и авторизации и на другие темы. За последние три года Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве провела учебные занятия по различным аспектам кибербезопасности для более чем 4500 человек.

В рамках исследования технических мер проводятся мероприятия, посвященные раннему обнаружению, сигнализации и оповещению. С этой целью в Турции разработаны системы обнаружения и предупреждения. Эти системы играют огромную роль в повышении уровня национальной кибербезопасности в Турции.

Несколько турецких организаций, учреждений, университетов, неправительственных организаций и предприятий частного сектора также проводят по всей стране семинары, конференции и учебные курсы по вопросам кибербезопасности, защиты важнейших объектов инфраструктур и другим смежным темам.

Кроме того, ежегодно организуется День безопасного Интернета, в ходе которого проводятся информационные мероприятия по вопросу сознательного и безопасного использования Интернета. Начали функционировать консультативная Интернет-сеть и безопасный веб-сайт, благодаря которым семьи могут проконсультироваться по вопросам эффективного использования Интернета (https://www.guvenlinet.org.tr/).

Поскольку круг пользователей ИКТ расширился, привлекательной целью для киберзлоумышленников стали персональные данные или личная информация. Тема конфиденциальности и защиты персональных данных входит в число основных вопросов безопасности. Поэтому в 2016 году в целях защиты неприкосновенности частной жизни вступил в силу закон № 6698 о защите персональных данных.

Турция играет важную роль во многих организациях, либо являясь одним из членов-основателей, либо содействуя сотрудничеству в сфере кибернетической и информационной безопасности. В этой связи Турция придает большое значение обмену информацией с различными странами и организациями по широкому кругу вопросов. Национальная группа по реагированию на чрезвычайные ситуации в киберпространстве Турции 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 и Альянс по кибербезопасности за взаимный прогресс. С ноября 2015 года в качестве страны-спонсора Турция также принимает участие в работе Центра передового опыта НАТО по совместной киберзащите. Кроме того, продолжается двустороннее и многостороннее сотрудничество по вопросам кибербезопасности; например, с многими странами подписываются меморандумы о взаимопонимании. К тому же Турция активно содействует и участвует в исследовательской работе таких международных организаций, как НАТО, Организация Объединенных Наций, Организация по безопасности и сотрудничеству в Европе, Организация экономического сотрудничества и развития, Группа двадцати, Совет сотрудничества тюркоязычных государств и Центр по сотрудничеству в области безопасности (РАКВИАК) .

Еще один важный шаг на пути укрепления сотрудничества и обеспечения готовности состоит в проведении учений по кибербезопасности. Такие учения, проводимые на национальном и международном уровнях, способствуют усилению защиты киберпространства и проверке мер, которые необходимо принять

для противодействия потенциальным киберугрозам. С 2011 года Министерство транспорта и инфраструктуры четыре раза провело учения по кибербезопасности на национальном уровне и два раза на международном. Совсем недавно, 19 декабря 2019 года, в Анкаре (Турция) Министерство транспорта и инфраструктуры и Управление информационно-коммуникационных технологий совместно организовали международные учения по кибербезопасности «Киберщит 2019». Эти учения состоялись при поддержке МСЭ и Альянса по кибербезопасности за взаимный прогресс. Кроме того, Турция участвует в международных учениях по кибербезопасности, таких как «Сомкнутые щиты НАТО», «Киберкоалиция НАТО» и учения НАТО по урегулированию кризисов, а также вносит вклад в проведение этих мероприятий.

Турция также ратифицировала Конвенцию о киберпреступности, которая охватывает различные преступления, например преступления, совершаемые при помощи сети Интернет и других компьютерных сетей, компьютерное мошенничество, детскую порнографию и нарушения в сфере сетевой безопасности; все эти киберпреступления сейчас отражены в национальном законодательстве Турции.

Чтобы обеспечить международный мир и безопасность в киберпространстве, нужно проводить дальнейшие исследования на основе расширения международного сотрудничества. Можно отчетливо увидеть, что международное право, а также нормы и правила, упомянутые в докладах Группы правительственных экспертов и соответствующих исследованиях, способствуют укреплению безопасности в киберпространстве.

Кроме того, работа по укреплению сотрудничества и содействию функционированию механизмов обмена информацией жизненно важна для борьбы с киберугрозами и должна учитываться в первоочередном порядке.

Следует также учитывать необходимость разработки руководств по обеспечению безопасности технологий нового поколения (Интернет вещей, сеть 5G, облачные технологии и т.д.). Руководства или базовые рекомендации по обеспечению безопасности технологий нового поколения, которые подготавливаются в сотрудничестве с государствами-членами, помогут повысить уровень готовности к новым киберугрозам, которые сопряжены с их применением. Как и другие исследования, касающиеся укрепления потенциала и разработки руководств, международные учения по кибербезопасности по-прежнему крайне важны для повышения уровня готовности и способности реагировать во всем мире на инциденты в киберпространстве.

Украина

[Подлинный текст на английском языке]
[29 мая 2020 года]

С тех пор как Российская Федерация развязала против Украины гибридную агрессию, возникли новые угрозы и вызовы, среди которых одно из важных мест занимает использование механизмов кибервоздействия в ущерб государственной безопасности Украины.

Украина по-прежнему твердо привержена международному праву в области использования информационно-коммуникационных технологий, а также в полной мере поддерживает выводы и рекомендации, содержащиеся в докладах Группы правительственных экспертов. Прежде всего, оно упоминает сохранение суверенного равенства государств, отказ от угрозы силой или ее применения

против территориальной целостности государств, невмешательство во внутренние дела других государств и уважение прав человека и основных свобод.

Чтобы работа по противодействию киберугрозам и правовому регулированию поведения в киберпространстве была организована эффективным образом, на фоне составления общих планов по формированию системы противодействия таким угрозам на государственном уровне был принят ряд нормативных актов, к главным из которых относятся Стратегия кибербезопасности Украины, утвержденная Советом национальной безопасности и обороны, постановление «О стратегии кибербезопасности Украины» (введено в действие указом № 96 президента Украины от 15 марта 2016 года) и закон «Об основных принципах обеспечения кибербезопасности Украины» от 5 мая 2017 года.

Отдельный механизм противодействия киберугрозам заключался в применении положений закона Украины «О санкциях» от 14 августа 2014 года, которые позволили организовать оперативное реагирование на выявленные угрозы путем применения ограничительных мер в отношении ряда юридических и физических лиц, причастных к совершению действий по нанесению ущерба национальной безопасности Украины.

Сегодня на Украине киберзащита государственных электронных информационных ресурсов и критически важной инфраструктуры осуществляется в соответствии с законом «Об основных принципах обеспечения кибербезопасности Украины». Определения полномочий, задач и функций субъектов кибербезопасности, закрепленные в этом законе, способствуют созданию комплексной системы обеспечения кибербезопасности.

В этой связи основным принципом разработки государственной политики в области кибербезопасности и киберзащиты является создание нормативной базы, соответствующей международным подходам и стандартам. Для выполнения этой задачи, в частности, были предприняты следующие шаги:

- принято постановление правительства Украины «Об утверждении общих требований к киберзащите объектов критической инфраструктуры»; подходы к кибербезопасности, определенные в настоящей резолюции, предусматривают учет требований международных стандартов в области информационной безопасности и реализацию директив Европейского союза, что делает государство равноправным участником в сфере глобальной безопасности;
- разработаны следующие проекты постановлений правительства Украины:
  - «Об утверждении порядка рассмотрения состояния киберзащиты важнейшей информационной инфраструктуры, государственных информационных ресурсов и информации, требования к защите которых установлены законом»;
  - «Об утверждении порядка определения объектов критической инфраструктуры»;
  - «Об утверждении порядка составления перечня объектов критической информационной инфраструктуры, включения объектов критической информационной инфраструктуры в государственный реестр объектов критической информационной инфраструктуры и их формирования и эксплуатации», принимая во внимание требования директивы (EU) 2016/1148 Европейского парламента и Совета «О мерах по обеспечению высокого общего уровня безопасности сетей и информационных систем на территории Союза»;

– «Об утверждении протокола о совместных действиях органов кибербезопасности, владельцев (руководителей) объектов критической информационной инфраструктуры при обнаружении, предотвращении, прекращении кибератак и киберинцидентов, а также при ликвидации их последствий».

В целях усовершенствования системы технической и криптографической защиты информации был представлен план реформ в сфере защиты информации путем адаптации законодательства Украины к требованиям законодательства Европейского союза; для реализации этого плана был разработан проект закона Украины «Об информационной безопасности и информационно-коммуникационных системах».

Одним из ключевых элементов эффективного развития национальной системы кибербезопасности является обзор состояния кибербезопасности. Результаты обзора послужат основой для разработки новой национальной стратегии кибербезопасности или корректировки существующей стратегии, совершенствования нормативной базы органов кибербезопасности, финансирования мероприятий по киберзащите государственных информационных ресурсов и важнейшей инфраструктуры, совершенствования системы подготовки кадров в области кибербезопасности, разработки новых подходов к формированию государственно-частного сотрудничества в этой сфере, усиления информационного обмена между субъектами кибербезопасности и их взаимодействия в решении вопросов безопасности.

Кроме того, в целях укрепления информационной безопасности и развития международного сотрудничества в этой области Государственная служба специальной связи предусматривает следующие меры:

- функционирование Группы реагирования на компьютерные инциденты Украины, которая аккредитована Форумом групп реагирования на инциденты в киберпространстве и взаимодействует с другими группами из 96 государств;
- государственный контроль за состоянием защиты в киберпространстве и технической защиты государственных информационных ресурсов и информации, требование о защите которых установлено законом;
- участие во встречах национальных координаторов, использующих Сеть связи Организации по безопасности и сотрудничеству в Европе (ОБСЕ);
- информирование общественности и проведение практических семинаров по вопросам кибербезопасности для субъектов национальной системы кибербезопасности;
- взаимодействие с правоохранительными органами и своевременное информирование о кибератаках;
- координация, организация и осуществление проверки коммуникационных и технологических систем критически важных объектов инфраструктуры, а также проверки уровня информационной безопасности в соответствии с государственным стандартом Украины ISO/IEC 27001: 2015.

Учитывая современные вызовы и угрозы, в сфере киберзащиты Украины внедряются правовые механизмы, нацеленные на следующее:

- усиление безопасности сетевых и информационных систем, основная цель которых должна заключаться в эффективной защите информации и данных, обеспечение стабильности сетей и систем и их бесперебойного функционирования, а также эффективность работы по обнаружению,

реагированию и минимизации издержек на восстановление после инцидентов в киберпространстве;

- внедрение системы управления рисками;
- создание условий для предоставления ресурсов, в том числе людских ресурсов в сфере кибербезопасности;
- укрепление оперативной и кибернетической устойчивости критически важных объектов инфраструктуры;
- создание системы резервирования государственных информационных ресурсов и обеспечение защиты технологической информации, необходимой для функционирования критически важных объектов инфраструктуры;
- участие в работе Комитета по общим критериям путем присоединения к соответствующему соглашению (Соглашение о признании сертификатов соответствия общим критериям в сфере безопасности информационных технологий), которое обеспечит включение сертифицированной на Украине продукции в реестр, признаваемый странами Европейского союза и другими странами, играющими в этой области ведущую роль;
- обеспечение строгого соблюдения требований законодательства в области защиты государственных информационных ресурсов и криптографическо-технической защиты информации, включая защиту персональных данных, руководителями органов управления критически важными объектами информационной инфраструктуры;
- использование возможностей государственно-частного партнерства и взаимодействия заинтересованных сторон для решения вопросов кибероборо-ны и кибербезопасности;
- повышение уровня культуры поведения в Интернете;
- активное участие в соответствующих инициативах международного сообщества и вступление в соответствующие структуры ведущих международных организаций.

В период 2015–2020 годов Совет национальной безопасности и обороны Украины ежегодно принимал решения о применении персональных специальных экономических и других ограничительных мер (санкций), которые проводились в жизнь на основании соответствующих указов президента Украины.

В добавление к вышесказанному следует отметить, что Служба безопасности Украины как одна из основных структур, отвечающих за обеспечение кибербезопасности, в соответствии со своей сферой компетенции, определенной законодательством, принимает меры по совершенствованию внутренней нормативно-правовой базы по вопросам киберпространства. В частности, на регулярной основе проводится работа по определению нормативных актов, необходимых для реализации закона «Об основных принципах обеспечения кибербезопасности Украины».

Принимаются меры по внесению положений закона «Об основных принципах обеспечения кибербезопасности Украины» в нормативно-правовую базу, регулирующую деятельность Службы безопасности Украины.

Однако на сегодняшний день, несмотря на эти меры, вопрос совершенствования нормативно-правовой базы в области информационной и кибернетической безопасности сохраняет свою актуальность.

В частности, ряд законодательных инициатив о Службе безопасности, которые рассматривались комитетами Верховной Рады предыдущего созыва, еще не рассмотрены украинскими парламентариями (ужесточение уголовной ответственности за киберпреступность, разделение следственных полномочий между Службой безопасности и Национальной полицией, а также установление ответственности за несоблюдение правил).

Положения Конвенции о киберпреступности не были выполнены в полном объеме.

Конвенция Совета Европы о киберпреступности от 23 ноября 2001 года была ратифицирована Верховной Радой Украины в сентябре 2005 года. Положения Конвенции предусматривают уголовную ответственность за следующие преступления против конфиденциальности, неприкосновенности и сохранности компьютерных данных и систем: незаконный доступ, несанкционированый перехват, воздействие на информацию, вмешательство в работу систем и неправомерное использование средств. То есть эти положения Конвенции охватывают преступления, совершаемые против бесперебойного функционирования важнейшей инфраструктуры.

Однако в настоящее время ряд положений Конвенции о киберпреступности не внесены в национальное законодательство, что ограничивает деятельность правоохранительных органов по выявлению и предупреждению киберпреступлений. В частности, необходимо внести положения Конвенции о киберпреступности, которые касаются оперативного обеспечения сохранности компьютерных данных, оперативного обеспечения сохранности и частичного раскрытия информации о трафике, порядка представления, поиска и изъятия хранящихся компьютерных данных и сбора информации о трафике в реальном времени (статьи 16–20). Кроме того, необходимо внести изменения в уголовно-процессуальный кодекс Украины, с тем чтобы ввести отдельную категорию доказательств, а именно цифровые доказательства в уголовном судопроизводстве.

В настоящее время представители Службы безопасности Украины в рабочей группе Комитета Верховной Рады по вопросам правоохранительной деятельности работают над проектом закона Украины «О внесении изменений в некоторые законодательные акты по вопросам соблюдения Конвенции о киберпреступности», с тем чтобы стандартизировать положения этой конвенции в законодательстве Украины, усовершенствовать положения уголовно-процес-суального кодекса Украины и создать эффективный правовой механизм борьбы с киберпреступностью, в том числе:

- предоставить руководителям оперативного подразделения, следователю и прокурору полномочия давать обязательные указания владельцам компьютерных данных (операторам и провайдерам связи, другим юридическим и физическим лицам) в отношении оперативного обеспечения сохранности компьютерных данных, необходимых для раскрытия преступления, на срок до 90 дней;

- установить требования по предоставлению операторам и провайдерам связи по запросу правоохранительных органов информации, необходимой для идентификации провайдеров услуг и маршрута, по которому была передана информация;

- внедрить эффективный механизм использования доказательств в электронной (цифровой) форме в уголовном судопроизводстве;

- внести изменения в уголовно-процессуальный кодекс Украины, закон «О телекоммуникациях» и проект закона «Об электронных коммуникациях», с

тем чтобы обеспечить создание правового механизма для временного ограничения доступа к информации или компьютерным данным, размещенным на определенном (идентифицированном) информационном ресурсе (сервисе), и определить порядок его внедрения.

4 февраля 2020 года Верховная Рада Украины отозвала проект закона «Об электронных коммуникациях» (рег. № 2264), к которому Служба безопасности Украины направила комментарии и предложения через Комитет Верховной рады Украины по вопросам цифровой трансформации в конце 2019 года.

5 февраля 2020 года в Верховной Раде Украины за № 3014 был зарегистрирован одноименный законопроект («Об электронных коммуникациях») и действовала почти идентичная авторская группа. Согласно предварительному анализу, в новом проекте правового акта также не содержится положений, которые способствовали бы полному осуществлению положений Конвенции о киберпреступности.

В 2020 году для решения актуальных вопросов в сфере кибербезопасности Служба безопасности Украины поддержала внесение законодательной инициативы о рассмотрении ряда законопроектов Верховной Радой девятого созыва. Принятие этих законопроектов заложит правовую основу для деятельности Службы безопасности в соответствии с законом «Об основных принципах обеспечения кибербезопасности Украины».

В частности, имеется законодательное разграничение между следователями Национальной полиции и органами безопасности при расследовании преступлений, совершенных с использованием компьютеров, системных и компьютерных сетей, телекоммуникационных сетей, государственных информационных ресурсов и критически важной информационной инфраструктуры, а за совершение этих преступлений ужесточается ответственность.

Выполнение задач по предупреждению, выявлению, пресечению и раскрытию преступлений против мира и безопасности человечества, совершенных в киберпространстве, и осуществление контрразведывательных и следственных мероприятий, направленных на борьбу с кибертерроризмом и кибершпионажем, обусловливают необходимость внесения изменений в закон «О контрразведывательной деятельности», с тем чтобы дополнить функции и полномочия структур, подразделений и сотрудников Службы безопасности Украины.

Кроме того, на законодательном уровне не разработаны принципы и указания для создания государственной системы защиты важнейшей инфраструктуры, а на уровне подзаконных актов не определено понятие критически важной инфраструктуры государства (пока не удалось установить ни перечень объектов важнейшей инфраструктуры, ни перечень объектов важнейшей информационной инфраструктуры).

В 2019 году правительство утвердило Общие требования к киберзащите критически важных объектов инфраструктуры (постановление кабинета министров Украины от 19 июня 2019 года № 518). Данный правовой акт является недействительным в случае отсутствия Государственного перечня критически важной инфраструктуры и Перечня критической информационной инфраструктуры, существование которых предусмотрено законом «Об основных принципах обеспечения кибербезопасности Украины».

Неопределенность в отношении критически важной инфраструктуры государства усложняет выполнение задач по обеспечению кибербезопасности, возложенных на Службу безопасности Украины и другие отвечающие за кибербезопасность структуры.

Необходимость обеспечения разработки и принятия закона «О критически важной инфраструктуре и ее защите», а также ускоренного принятия указов кабинета министров Украины, направленных на осуществление положений закона «Об основных принципах обеспечения кибербезопасности Украины», была подчеркнута Комитетом Верховной рады Украины по вопросам цифровой трансформации в ходе состоявшегося 23 декабря 2019 года заседания, которое было посвящено вопросу национальной кибербезопасности и кибероборонe Украины, в том числе в сфере критически важной инфраструктуры.

Вопрос практики применения закона «Об основных принципах обеспечения кибербезопасности Украины» и принятия нормативно-правовых актов, необходимых для его реализации, был отдельно рассмотрен на заседании Комитета Верховной рады по вопросам цифровой трансформации, которое состоялось 19 февраля 2020 года.

Сохраняет актуальность проблема отсутствия положений, направленных на снижение уровня острой зависимости национальных учреждений, организаций и предприятий от программного обеспечения иностранного происхождения, которое может намеренно иметь уязвимые места и не отраженные в документации функции.

По мнению специалистов Службы безопасности Украины, для этого необходимо разработать национальную программу импортозамещения в области информатизации и комплекс мер по поддержке отечественных производителей программного обеспечения, а также создать:

- реестр проверенных поставщиков программного обеспечения для критически важных объектов информационной инфраструктуры, а также подготовить процедуры их включения/исключения из указанного реестра;
- реестр запатентованного программного обеспечения, рекомендованного для использования на критически важных объектах информационной инфраструктуры;
- национальное хранилище бесплатных программных средств, а также активизировать усилия по реализации государственных программ, касающихся их передачи государственным органам и регулирования порядка их использования.

Кроме того, в целях установления законодательной процедуры незамедлительного и эффективного реагирования на существующие и потенциальные угрозы национальным интересам и безопасности Украины в сфере информационно-коммуникационных технологий, в закон «О санкциях» необходимо ввести соответствующие изменения: установить ограничения на использование на критически важных объектах инфраструктуры программного обеспечения (в том числе антивирусного) и телекоммуникационного оборудования любой формы собственности, которое было разработано или изготовлено хозяйствующими единицами страны-агрессора.

Еще одним фактором, оказывающим негативное воздействие, является несовершенство национального законодательства в части отсутствия законодательно закрепленного механизма для блокирования доступа пользователей к Интернет-ресурсам и для удаления сообщений, содержащих незаконно полученную информацию.

Следует также отметить, что Служба безопасности Украины поддерживает международное сотрудничество в целях укрепления информационной и кибернетической безопасности. В Стратегии кибербезопасности Украины указаны следующие основные приоритеты и направления деятельности:

- укрепление международного сотрудничества в области кибербезопасности;
- поддержка международных инициатив в сфере кибербезопасности, которые отвечают национальным интересам Украины;
- углубление сотрудничества Украины с Европейским союзом и Организацией Североатлантического договора (НАТО) в целях укрепления потенциала Украины в сфере кибербезопасности;
- участие в работе по укреплению доверия в киберпространстве под эгидой ОБСЕ.

В частности, Служба безопасности Украины в рамках своей компетенции участвует в совместном проекте «КиберВосток», который инициирован Европейским союзом и Советом Европы для стран — участниц программы «Восточное партнерство» и направлен на реализацию законодательных и директивных решений по осуществлению положений Будапештской конвенции о киберпреступности. Проект «КиберВосток» осуществляется Генеральным директоратом Европейского союза по соседству и переговорам о расширении совместно с Бюро программ по киберпреступности при Совете Европы.

Подчеркивая важность информирования международных партнеров о последних достижениях Украины в сфере кибербезопасности и реализации определенных мер по укреплению доверия в соответствии с решениями Постоянного совета ОБСЕ № 1039, 1106, 1202 в области ИКТ и их применения, представители Службы безопасности Украины обычно участвуют в заседаниях Неофициальной рабочей группы ОБСЕ по ИКТ. Кроме того, в рамках соблюдения меры по укреплению доверия № 8, которая изложена в решении № 1202, Служба безопасности Украины назначила координатора, который на профессиональном уровне осуществляет деятельность в рамках плановых и внеплановых проверок связи.

Служба безопасности Украины также участвует в проекте ОБСЕ, основная цель которого заключается в осуществлении тщательного анализа национальной структуры управления в сфере кибербезопасности и реализации украинских мер по укреплению доверия в сфере ИКТ и кибербезопасности, предусмотренных решением № 1202.

Кроме того, с учетом возложенных на Службу безопасности Украины задач и при поддержке Целевого фонда НАТО и Украины по кибербезопасности было приобретено необходимое оборудование, а при Службе безопасности Украины был создан оперативный центр по кибербезопасности, который решает следующие задачи:

- предупреждение, обнаружение, пресечение и выявление преступлений против мира и безопасности человечества, совершаемых в киберпространстве;
- проведение контрразведывательных и следственных мероприятий, направленных на борьбу с кибертерроризмом и кибершпионажем;
- проверка готовности критически важных объектов инфраструктуры к возможным кибератакам и киберинцидентам;
- противодействие киберпреступности, которая по своим последствиям может угрожать жизненно важным интересам государства;
- расследование киберинцидентов и кибератак на государственные электронные информационные ресурсы и критически важную информационную инфраструктуру;

• обеспечение реагирования на киберинциденты в сфере государственной безопасности.

Служба безопасности Украины также инициировала сотрудничество по обмену информацией об угрозах, атаках и инцидентах в киберпространстве; при этом используется платформа по обмену информацией о вредоносных программах и угрозах «Украинское преимущество», которая служит общественной площадкой для сотрудничества Службы безопасности Украины с критически важными объектами инфраструктуры, предприятиями, учреждениями и организациями, независимо от их форм собственности, а также физическими лицами в вопросах повышения уровня безопасности в интересах пользователей информации, телекоммуникаций и информационно-телекоммуникационных систем, защиту которых они уполномочены обеспечивать в силу заключенных договоров или других правовых оснований.

Объединенные Арабские Эмираты

[Подлинный текст на арабском языке]
[31 мая 2020 года]

Национальный доклад об усилиях Объединенных Арабских Эмиратов по укреплению информационной безопасности и развитию международного сотрудничества в области кибербезопасности

Введение

Объединенные Арабские Эмираты придают кибербезопасности огромное значение. Использование информационно-коммуникационных технологий (ИКТ) для отражения атак, которые создают серьезную угрозу для инфраструктуры, государственных служб и отдельных лиц, — залог поддержания национальной безопасности страны. Поэтому Объединенные Арабские Эмираты стремятся создать комплексную систему для обеспечения безопасности жизненно важных секторов, укрепления доверия среди пользователей и стимулирования инновационной деятельности.

Усилия, предпринимаемые на национальном уровне для укрепления информационной безопасности

Страна приступила к осуществлению национальной стратегии кибербезопасности, с тем чтобы сформировать безопасную и гибкую цифровую среду, которая создавала бы возможности для реализации частных устремлений и роста компаний. По своим целям стратегия охватывает пять основных направлений:

1. создать всеобъемлющую нормативно-правовую базу для борьбы с киберпреступностью, защиты существующих и новейших технологий и предоставления малым и средним предприятиям возможности защитить себя от киберугроз;

2. разработать комплексную программу повышения осведомленности и укрепления потенциала в области кибербезопасности в целях поощрения безопасных методов использования технологий и развития у сотрудников по вопросам кибербезопасности навыков эффективно реагировать на нападения и обеспечивать безопасность систем и услуг;

3. разработать эффективный национальный план, позволяющий оперативно и слаженно реагировать на инциденты, связанные с кибербезопасностью, в масштабах всей страны;

4. защищать цифровую инфраструктуру жизненно важных секторов;

5. укреплять местные и глобальные партнерства в области кибербезопасности.

В 2006 году Объединенные Арабские Эмираты приняли закон о борьбе с преступлениями в сфере информационных технологий, который содержит многочисленные положения о защите частных материалов, публикуемых и распространяемых с помощью ИКТ в средствах массовой информации, и о наказании за неправомерное использование таких средств массовой информации.

На протяжении ряда лет Объединенные Арабские Эмираты также осуществляли многочисленные программы и инициативы, направленные на укрепление кибербезопасности, включая создание национальной Группы реагирования на чрезвычайные ситуации в компьютерной сфере. Эта группа предоставляет правительственным учреждениям ряд услуг, таких как круглосуточный мониторинг и инспектирование инфраструктуры в целях выявления любой необычной деятельности и непосредственного реагирования на атаки; эффективное реагирование на инциденты в сфере кибербезопасности; а также оценка уровня безопасности веб-сайтов и приложений для мобильных телефонов в целях устранения уязвимых мест, которые могут использоваться в неблаговидных целях или привести к утечке информации. На различных платформах, включая веб-сайт, социальные сети и список рассылки, Группа также предоставляет государственным учреждениям и частным лицам регулярные указания по вопросам безопасности и сообщения о серьезных кибератаках.

Чтобы во всех жизненно важных секторах страны применялись передовые методы обеспечения кибербезопасности, была создана система информационной безопасности, устанавливающая контрольные требования в отношении повышения минимального уровня защиты средств и вспомогательных систем информационной безопасности.

Усилия необходимо активизировать не только для совершенствования стратегий и технических систем, но и для повышения профессионального уровня сотрудников; это нужно для того, чтобы повысить их информированность о том, как в интересах страны и семьи конструктивно и безопасно использовать ИКТ, превратив их в первую линию защиты от опасных кибератак. С учетом этого было начато осуществление национальной программы повышения осведомленности и укрепления потенциала в сфере кибербезопасности, с тем чтобы укрепить в обществе культуру кибербезопасности и повысить национальный уровень компетентности в сфере кибербезопасности. В рамках инициативы «КиберПро» специалисты по кибербезопасности проходят месячные курсы обучения. Также была создана виртуальная академия, предлагающая курсы в той же области. Для различных слоев общества периодически проводятся общественно-информационные кампании и мероприятия.

В целях защиты детей в сети Интернет был создан анимационный герой Салим, благодаря чему удалось добиться больших успехов в деле информирования детей в доступной и занимательной форме о принципах безопасного использования технологий. В дополнение к учебной программе по цифровой безопасности, разработанной в сотрудничестве с Министерством образования, и запуску веб-сайта о Салиме были организованы тысячи интерактивных семинаров для обучения детей с помощью историй, в которых они являются главными действующими лицами. Эти мероприятия также позволили вовлечь детей в информационно-просветительскую работу в рамках инициативы «Послы кибербезопасности», которая дает им возможность информировать сверстников и содействовать проявлению в этом вопросе безопасного и здравого подхода.

Усилия по укреплению международного сотрудничества в области кибербезопасности

Объединенные Арабские Эмираты хорошо понимают, что для достижения оптимального уровня кибербезопасности и способности реагировать на атаки и риски требуются международное сотрудничество и серьезный настрой. Поэтому наша страна стремится принимать активное участие во всех международных форумах по вопросам кибербезопасности, некоторые из которых упоминаются ниже.

Объединенные Арабские Эмираты являются членом Международного союза электросвязи (МСЭ) и совместно с другими государствами-членами работают над поиском решений и выявлением передовых методов обеспечения кибербезопасности в рамках соответствующих исследовательских комиссий и рабочих групп. Отрадно, что ряд специалистов из нашей страны занимают в Союзе ключевые посты, например пост руководителя Рабочей группы Совета МСЭ по защите детей в Интернете, что подчеркивает готовность нашей страны поддерживать глобальные усилия по решению этих важных вопросов.

По линии Группы реагирования на чрезвычайные ситуации в компьютерной сфере Объединенные Арабские Эмираты представлены в Совете Группы реагирования на компьютерные инциденты при Организации исламского сотрудничества, где наша страна содействует повышению осведомленности о кибербезопасности путем разработки программ, руководств и других важнейших материалов об угрозах безопасности для учреждений и людей. Группа реагирования на чрезвычайные ситуации в компьютерной сфере также принимает активное участие в работе Арабского регионального центра кибербезопасности и Комитета национальных центров реагирования на компьютерные инциденты, действующего при Совете сотрудничества государств Залива.

Помимо участия в работе международных форумов и международных организаций Объединенные Арабские Эмираты стремятся укреплять двустороннее сотрудничество в области кибербезопасности с дружественными странами путем подписания меморандумов о взаимопонимании и соглашений, регулирующих обмен информацией и экспертным опытом между странами и взаимодействие в деле борьбы с кибератаками.

Мнения относительно содержания концепций, упомянутых в докладах Группы правительственных экспертов

Объединенные Арабские Эмираты хотели бы поблагодарить Группу правительственных экспертов за ее доклады о достижениях в сфере информатизации и телекоммуникаций в контексте международной безопасности. Объединенные Арабские Эмираты согласны с выводами Группы о том, что государствам важно стремиться предотвращать вредную практику в сфере ИКТ, сотрудничать в деле реагирования на кибератаки, поддерживать диалог на основе транспарентности и взаимодействия, содействовать глобальному развитию цифровой инфраструктуры и консультироваться по вопросам разработки законодательства, стратегий и систем в области кибербезопасности.

III. Ответы, полученные от межправительственных организаций

Европейский союз

[Подлинный текст на английском языке]
[20 мая 2020 года]

Киберпространство, включая глобальный открытый Интернет, стало одной из основ нашего общества. Оно служит платформой, которая обеспечивает связь и экономический рост. Европейский союз и его государства-члены поддерживают глобальное, открытое, стабильное, мирное и безопасное киберпространство, где в целях обеспечения социального благосостояния, экономического роста, процветания и стабильности свободного и демократического общества в полной мере соблюдаются права человека, основные свободы и верховенство права.

По мере того как Интернет все заметнее входит в нашу жизнь, в киберпространстве возникает ряд тех же самых проблем, с которыми мы сталкиваемся в физическом мире. В международном контексте некоторые государства, по-видимому, восприняли концепцию киберпространства, которая предполагает высокую степень государственного контроля и вызывает озабоченность в связи с нарушениями прав человека и основных свобод. Кроме того, отмечается тревожная активизация вредоносных действий в киберпространстве со стороны государственных и негосударственных субъектов. Европейский союз и его государства-члены регулярно выражают озабоченность по поводу таких вредоносных действий, которые подрывают основанный на правилах международный порядок и повышают риск возникновения конфликтов.

а) Усилия, предпринимаемые 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 кибербезопасности — важнейший элемент поддержания международного мира и стабильности путем снижения риска возникновения конфликтов и путем решения проблем, связанных с цифровизацией экономики и общества. Глобальная кибербезопасность снижает способность потенциальных злоумышленников использовать информационно-коммуникационные технологии (ИКТ) в неблаговидных целях и укрепляет способность государств эффективно реагировать на киберинциденты и преодолевать их последствия.

Стратегия кибербезопасности «Открытое, безопасное и защищенное киберпространство»[12], а также нижеупомянутые другие последующие программные документы излагают всеобъемлющее видение Европейского союза в отношении того, как лучше всего предотвращать сбои и атаки в киберпространстве и реагировать на них. Они направлены на укрепление ценностей Европейского союза и формирование условий для роста цифровой экономики. Некоторые конкретные действия 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[13] Совет Европейского союза подчеркнул важность дальнейшей разработки и реализации общего и всеобъемлющего подхода Европейского союза к кибердипломатии, который содействует соблюдению прав человека и уважению основных ценностей Европейского союза, обеспечивает свободу выражения мнений, способствует гендерному равенству, стимулирует экономический рост, предусматривает борьбу с киберпреступностью, смягчает угрозы кибербезопасности, предотвращает конфликты и обеспечивает стабильность в сфере международных отношений. Европейский союз также призывает к укреплению многосторонней модели управления Интернетом и к активизации усилий по наращиванию потенциала в третьих странах. Кроме того, Европейский союз признает важность взаимодействия с ключевыми партнерами и международными организациями. Европейский союз также подчеркивает, что применение существующего международного права в области международной безопасности, актуальность норм поведения и важность управления Интернетом — это неотъемлемая часть общего и всеобъемлющего подхода Европейского союза к кибердипломатии.

По результатам обзора Стратегии кибербезопасности 2013 года Европейский союз еще сильнее 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»[14] были определены масштаб задач и комплекс мер, предусмотренных на уровне Европейского союза и призванных обеспечить его более надежную подготовку к решению постоянно растущих проблем в сфере кибербезопасности.

Озабоченность постоянно растущими проблемами в сфере кибербезопасности послужила стимулом к тому, чтобы разработать механизм совместного дипломатического реагирования Европейского союза на вредоносную деятельность в кибрепространстве — инструментарий кибердипломатии[15]. Растущая способность и готовность государственных и негосударственных субъектов добиваться своих целей с помощью вредоносной деятельности в кибрепространстве должна вызывать у международного сообщества озабоченность. Такая

---

[12] 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».

[13] 6122/15. Заключения Совета относительно кибердипломатии.

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

[15] 10474/17. Заключения Совета относительно механизма совместного дипломатического реагирования Европейского союза на вредоносную деятельность в киберпространстве («Инструментарий кибердипломатии»).

деятельность может выражаться в деяниях, являющихся противоправными по международному праву, и может приводить к дестабилизирующим и многоуровневым последствиям, сопряженным с повышенным риском возникновения конфликта. Европейский союз и его государства-члены привержены урегулированию международных споров в киберпространстве мирными средствами. В этой связи механизм совместного дипломатического реагирования Европейского союза вписывается в подход Европейского союза к кибердипломатии, который способствует предотвращению конфликтов, смягчению угроз в сфере кибербезопасности и усилению стабильности в области 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, сдерживанию и учету злонамеренных действий и стремятся в этой связи к укреплению международного сотрудничества.

Международная политика Европейского союза по вопросам киберпространства поощряет уважение основных ценностей Европейского союза, определяет нормы ответственного поведения и содействует применению существующих международных законов в киберпространстве, оказывая помощь странам, не входящим в состав Европейского союза, в наращивании потенциала в области кибербезопасности и стимулируя международное сотрудничество по вопросам киберпространства.

b) 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 (ИКТ) как государственными, так и негосударственными субъектами, а также увеличением числа случаев хищения интеллектуальной собственности в киберпространстве. Такое поведение подрывает экономический рост, ставит под угрозу защищенность, безопасность и стабильность мирового сообщества и может привести к дестабилизирующим и многоуровневым последствиям с повышенным риском возникновения конфликта.

В последнее время по мере продолжения пандемии коронавирусной инфекции (COVID-19) Европейский союз и его государства-члены отслеживают в киберпространстве угрозы и вредоносные действия, направленные против основных операторов в государствах-членах и их международных партнеров, в том числе в сфере здравоохранения. Европейский союз и его государства-члены осуждают эту вредоносную деятельность в киберпространстве и подчеркивают

свою неизменную поддержку усилий по укреплению глобальной кибербезопасности.

Любые попытки помешать функционированию критически важных объектов инфраструктуры неприемлемы и могут поставить под угрозу жизнь людей. Все субъекты должны воздерживаться от проведения безответственной и дестабилизирующей деятельности в киберпространстве. Как 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 с ее территории подобную деятельность. 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 запросы другого государства о сдерживании вредоносной кибердеятельности, исходящей с их территории.

Кроме того, как с учетом уникального характера ИКТ признается в предыдущих докладах группы правительственных экспертов, подход Европейского союза к борьбе с киберугрозами в контексте международной безопасности должен оставаться технологически нейтральным. Это соответствует концепции и признанию Организации Объединенных Наций о том, что существующее международное право применимо к новым областям, включая использование новых технологий.

Европейский союз и его государства-члены могут только поддерживать развитие и использование технологий, систем или услуг, которые существуют благодаря ИКТ и при полном соблюдении применимого международного права и норм, в частности Устава Организации Объединенных Наций, а также международного гуманитарного права и вытекающих из него принципов и прав человека.

Как международное право применяется в сфере использования 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. Кроме того, Европейский союз и его государства-члены подтверждают применимость существующего международного права к поведению государств в киберпространстве, как это признано в докладах Группы правительственных экспертов за 2010, 2013 и 2015 годы, а также принципов, установленных в пунктах 28 a) –28 f) доклада 2015 года.

Международное право, в том числе международное гуманитарное право, включающее 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 во время конфликтов. Европейский союз подчеркивает свою убежденность в том, что международное

право не обуславливает то или иное поведение, но устанавливает 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 сети Интернет, так и в реальной жизни. Европейский союз и его государства-члены приветствуют тот факт, что значение этих принципов также подтвердили Совет по правам человека[16] и Генеральная Ассамблея.

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 международная правовая база уже существует.

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

Мы продолжаем поддерживать предпринимаемые усилия по содействию применению действующего международного права в киберпространстве, в том числе по обмену информацией и передовым опытом в области применения существующего международного права в киберпространстве. Мы обязуемся и далее информировать о национальных позициях в отношении того, как международное право применяется к использованию ИКТ государствами, поскольку оно способствует транспарентности и содействует глобальному пониманию национальных подходов; это имеет основополагающее значение для поддержания долгосрочного мира и стабильности и снижения риска возникновения конфликтов в результате совершаемых в киберпространстве действий. Дальнейшее внимание следует уделять повышению осведомленности о применимости существующего международного права в качестве средства для 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 стимулировать работу, неоднократно одобренную Генеральной Ассамблеей, в частности в ее резолюции 70/237, и дальнейшее осуществление этих 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 существующими нормами международного права, а также придерживаться добровольных норм, правил и принципов ответственного поведения государства и их реализации в киберпространстве, как это было сформулировано в ряде докладов Группы правительственных экспертов в 2010, 2013 и 2015 годах. Мы считаем, что для практического продвижения вперед нужно стимулировать расширение сотрудничества и повышение прозрачности для обмена передовым опытом, в том числе по вопросам порядка применения существующих норм Группы правительственных экспертов, через соответствующие инициативы и структуры, такие как региональные организации и учреждения, в

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

целях содействия повышению осведомленности и эффективного осуществления согласованных норм ответственного поведения государств.

Меры по укреплению доверия

Разработка эффективных механизмов государственного сотрудничества и взаимодействия в киберпространстве — важнейший компонент деятельности по предотвращению конфликтов. Региональные форумы зарекомендовали себя в качестве подходящей платформы, призванной формировать пространство для диалога и сотрудничества между субъектами с общими проблемами и интересами в целях эффективного решения проблем с региональной точки зрения.

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 (ОБСЕ), Регионального форума Ассоциации государств Юго-Восточной Азии (АСЕАН), Организации американских государств (ОАГ) и других региональных учреждений повысят предсказуемость поведения государств и снизят риск неправильного толкования, эскалации наряженности и существования конфликтов, которые могут возникнуть 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 их навыков и потенциала в области борьбы с инцидентами в киберпространстве, а также поддерживают инициативы, способствующие обмену передовым опытом, будь то в рамках 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 укрепления потенциала в третьих странах.