ОБНОВЛЕННАЯ КОНЦЕПЦИЯ КОНВЕНЦИИ ОРГАНИЗАЦИИ ОБЪЕДИНЕННЫХ НАЦИЙ ОБ ОБЕСПЕЧЕНИИ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Предложение Российской Федерации

Соавторы: Республика Беларусь, Боливарианская Республика Венесуэла, Корейская Народно-Демократическая Республика, Республика Никарагуа, Сирийская Арабская Республика

Информационно-коммуникационные технологии являются технологиями двойного назначения *(A/RES/75/240, PP8)* и потенциально могут быть использованы в целях, несовместимых с задачами обеспечения международного мира, безопасности и стабильности, негативно воздействовать на целостность инфраструктуры государств в ущерб их безопасности как гражданской, так и военной *(A/RES/76/19, PP5)*. Ряд государств занимается наращиванием потенциала в сфере информационно-коммуникационных технологий в военных целях *(A/RES/76/19, PP3)*. Использование этих технологий в будущих конфликтах между государствами становится более вероятным *(A/RES/76/19, PP3)*.

Повышается потребность в мирном использовании информационно-коммуникационных технологий, их применения в интересах всеобщего блага человечества и дальнейшего социально-экономического развития государств.

Растет необходимость заключения государствами в рамках ООН юридически обязательного многостороннего международного договора *(A/75/816, A/76/135, A/RES/76/19, PP10)*, который будет обеспечивать решение задачи предотвращения и урегулирования межгосударственных конфликтов в глобальном информационном пространстве, способствовать исключительно мирному использованию информационно-коммуникационных технологий и создавать основу для сотрудничества государств в данных целях.

Решение проблемы видится в принятии Конвенции ООН об обеспечении международной информационной безопасности (далее – Конвенция), регулирующей отношения государств по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий. Документ мог бы включать приведенные ниже положения, основанные в том числе на рекомендациях ежегодных резолюций Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной

безопасности», а также консенсусных докладов профильной Рабочей группы открытого состава (РГОС) ООН 2021 года и групп правительственных экспертов 2010, 2013, 2015 и 2021 годов.

I. Цели Конвенции

Принятие Конвенции способствовало бы формированию системы обеспечения международной информационной безопасности на основе равноправного сотрудничества между государствами в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий для достижения следующих целей:

1. предотвращение и урегулирование межгосударственных конфликтов в глобальном информационном пространстве, создающих или усугубляющих угрозу международному миру и безопасности, а также способных нарушить мир или спровоцировать акты агрессии *(A/RES/75/240, PP10)*;

2. укрепление доверия и развитие сотрудничества государств-членов ООН в сфере международной информационной безопасности в целях преодоления напряженности, возникшей в результате злонамеренного использования информационно-коммуникационных технологий *(A/RES/75/240, OP1)*;

3. содействие наращиванию потенциала государств в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий *(A/RES/75/240, OP1)*.

II. Основные угрозы международной информационной безопасности и влияющие на них факторы

При разработке Конвенции целесообразно исходить из следующих угроз международной информационной безопасности:

1. использование государствами информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности, общественной и экономической стабильности суверенных государств, вмешательства в их внутренние дела, а также осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира и безопасности (*резюме председателя РГОС 2021 г., A/75/816, п.20; доклад ГПЭ 2021 г., A/76/135, п.70; доклад ГПЭ 2015 г., A/70/174, п.71 (c); вклады Движения неприсоединения, Ирана, Китая*

в резюме председателя РГОС 2021 г., A/75/816; Правила поведения ШОС в области МИБ, A/69/723, п.3);

2. проведение компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру *(промежуточный доклад РГОС 2022 г., A/77/275, п.10; доклад ГПЭ 2021 г.)*;

3. монополизация отдельными государствами и/или при их содействии частными компаниями рынка информационно-коммуникационных технологий путем ограничения доступа других государств к передовым информационно-коммуникационным технологиям и усиления их технологической зависимости от доминирующих в сфере информатизации государств, увеличения цифрового неравенства *(Правила поведения ШОС в области МИБ, A/69/723, п.5)*;

4. выдвижение одними государствами против других государств необоснованных обвинений в организации и совершении противоправных деяний с использованием информационно-коммуникационных технологий, включая компьютерные атаки (*резюме председателя РГОС 2021 г., A/75/816, п.15; доклад ГПЭ 2021 г., A/76/135, п.71 (g); доклад ГПЭ 2015 г., A/70/174, п.28 (f)*);

5. использование информационных ресурсов, находящихся под юрисдикцией другого государства, без согласования с компетентными органами этого государства;

6. размещение в информационном пространстве государств в свободном доступе инструментов проведения компьютерных атак, инструкций по методам их организации и выработке практических навыков применения таких инструментов, координации соответствующих действий по проведению компьютерных атак;

7. использование информационно-коммуникационных технологий в ущерб основным правам и свободам человека, реализуемым в информационном пространстве, прежде всего праву человека на уважение его личной (частной) жизни *(A/RES/73/27, OP1.5; доклад ГПЭ 2015 г., A/70/174, п.13 (e))*;

8. включение в информационно-коммуникационные технологии недекларируемых возможностей, а также сокрытие производителями информации об уязвимостях в их продуктах *(A/RES/73/27, OP1.10, 1.11; доклад ГПЭ 2015 г., A/70/174, п.13 (i, g))*;

9. использование государствами своей информационной инфраструктуры для совершения международно-противоправных деяний, а также использование государствами посредников, в том числе

негосударственных субъектов, для совершения таких деяний *(A/RES/73/27, OP1.13; доклад ГПЭ 2015 г., A/70/174, п.13 (c))*;

10. распространение посредством информационно-коммуникационных технологий информации, наносящей вред общественно-политическим и социально-экономическим устоям, духовной, нравственной и культурной средам государств, а также создающей угрозы жизни и безопасности граждан;

11. невозможность точной идентификации источника компьютерных атак, обусловленная технологическими особенностями информационно-коммуникационных технологий, а также отсутствием организационных механизмов обеспечения деанонимизации информационного пространства, для совершения противоправных деяний.

III. Предотвращение и урегулирование межгосударственных конфликтов в глобальном информационном пространстве

Следующие принципы и предложения могли бы лечь в основу положений Конвенции, регулирующих деятельность государств и определяющих их права и обязанности в части реализации задачи предотвращения и урегулирования конфликтов в глобальном информационном пространстве:

1. суверенное право каждого государства на обеспечение безопасности национального информационного пространства, установление норм и механизмов управления своим информационным и культурным пространством в соответствии с национальным законодательством *(A/RES/73/27, PP16, 18; A/RES/75/240, PP17, 19)*;

2. суверенное равенство и одинаковые права, а также одинаковые обязанности государств независимо от различий экономического, социального, политического или иного характера в рамках системы обеспечения международной информационной безопасности *(A/RES/75/240, PP17, 19; доклад ГПЭ 2021 г., A/76/135, п.70, 71 (b))*;

3. воздержание в международных отношениях от угрозы силой или ее применения в отношении информационно-коммуникационной инфраструктуры другого государства или в качестве средства разрешения конфликтов *(A/RES/73/27, PP16; A/RES/75/240, PP17; вклады Ирана, Китая в резюме председателя РГОС 2021 г., A/75/816)*;

4. недопущение использования информационно-коммуникационных технологий для подрыва и ущемления суверенитета, нарушения территориальной целостности и независимости государств (*резюме председателя РГОС 2021 г., A/75/816, п.20; доклад ГПЭ 2021 г., A/76/135, п.70)*;

5. отказ от использования информационно-коммуникационных технологий для вмешательства во внутренние дела суверенных государств *(доклад ГПЭ 2015 г., A/70/174, п.71 (c); вклады Ирана, Китая в резюме председателя РГОС 2021 г., A/75/816; Правила поведения ШОС в области МИБ, A/69/723, п.3)*;

6. недопустимость бездоказательных обвинений других государств в организации и совершении противоправных деяний с использованием информационно-коммуникационных технологий, включая компьютерные атаки, в том числе для последующего принятия различного рода ограничений в виде односторонних мер экономического воздействия и иных способов реагирования *(резюме председателя РГОС 2021 г., A/75/816, п.15; доклад ГПЭ 2021 г., A/76/135, п.71 (g); доклад ГПЭ 2015 г., A/70/174, п.28 (f))*;

7. урегулирование межгосударственных конфликтов путем переговоров, посредничества, примирения или иными мирными средствами по своему выбору, в том числе путем проведения консультаций с участием национальных органов государств, уполномоченных на решение задач в области обнаружения, предупреждения и ликвидации последствий компьютерных атак, а также реагирования на компьютерные инциденты *(доклад РГОС 2021 г., A/75/816, п.35)*;

8. полное и добросовестное выполнение государствами взятых на себя обязательств по обеспечению международной информационной безопасности *(вклад Канады в резюме председателя РГОС 2021 г., A/75/816)*;

9. отказ от принятия доктринальных документов и планов, нацеленных на провоцирование угроз и конфликтов в глобальном информационном пространстве, а также на создание напряженности в отношениях между государствами *(вклад Канады в резюме председателя РГОС 2021 г., A/75/816)*;

10. создание государствами механизмов для предотвращения компьютерных атак с их территории или с использованием информационной инфраструктуры, находящейся под их юрисдикцией, а также механизмов для взаимодействия между государствами в целях определения источника компьютерных атак, проведенных с их территории, противодействия этим атакам и ликвидации их последствий *(резюме председателя РГОС 2021 г., A/75/816, п.20; доклад ГПЭ 2021 г., A/76/135, п.22, 23)*;

11. недопустимость включения государствами и/или при их содействии недекларируемых возможностей в информационно-коммуникационные технологии и средства, а также сокрытие производителями информации об уязвимостях в их продуктах *(A/RES/73/27, OP1.10, 1.11; доклад ГПЭ 2015 г., A/70/174, п.13 (i, g))*;

12. недопустимость присвоения той или иной деятельности в сфере информационно-коммуникационных технологий государству лишь на основании происхождения этой деятельности с территории или объектов информационной инфраструктуры указанного государства и необходимость обоснования обвинений в организации и совершении противоправных деяний, выдвигаемых против государств (при этом государства должны изучить в случае инцидентов всю соответствующую информацию, в том числе более широкий контекст события, проблемы установления ответственности, а также характер и масштабы ответственности) *(A/RES/73/27, OP1.2; доклад ГПЭ 2021 г., A/76/135, п.71 (g); доклад ГПЭ 2015 г., A/70/174, п.13 (b))*;

13. недопустимость заведомого использования государствами своей территории для совершения международно-противоправных деяний с использованием информационно-коммуникационных технологий и задействования посредников, а также стремление к недопустимости использования территорий государств негосударственными субъектами для совершения таких деяний *(A/RES/73/27, OP1.13; доклад ГПЭ 2015 г., A/70/174, п.13 (c))*;

14. недопустимость заведомого осуществления и поддержки государствами деятельности в сфере использования информационно-коммуникационных технологий, 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 *(A/RES/73/27, OP1.6; доклад ГПЭ 2015 г., A/70/174, п.13 (f))*;

15. важность принятия государствами надлежащих мер для защиты собственной критически важной инфраструктуры от угроз в сфере использования информационно-коммуникационных технологий *(A/RES/73/27, OP 1.7; доклад ГПЭ 2015 г., A/70/174, п.13 (g))*;

16. отказ от заведомого осуществления и поддержки деятельности, призванной нанести ущерб информационным системам уполномоченных групп реагирования на компьютерные инциденты другого государства, а также от использования уполномоченных групп реагирования на компьютерные инциденты для осуществления злонамеренной международной деятельности *(A/RES/73/27, OP1.12; доклад ГПЭ 2015 г., A/70/174, п.13 (k))*;

17. содействие тому, чтобы частный сектор и гражданское общество имели важное значение в укреплении безопасности в сфере использования

информационно-коммуникационных технологий и самих информационно-коммуникационных технологий, включая безопасность всей системы производства и сбыта товаров и услуг в сфере информационно-коммуникационных технологий и информационной безопасности *(A/RES/73/27, OP1.13)*;

18. обеспечение осведомленности граждан, общественных и государственных органов, профильных структур и международных организаций о новых угрозах международной информационной безопасности и об имеющихся вариантах их предотвращения, а также повышение грамотности всех пользователей в сфере информационной безопасности;

19. отказ от использования информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве, прежде всего праву человека на уважение его личной (частной) жизни *(A/RES/73/27, OP1.5; доклад ГПЭ 2015 г., A/70/174, п.13 (e));*

20. уважение свободного выражения мнения каждого человека, включая свободу искать, получать и распространять информацию, при возможности введения ограничений, установленных законом, для защиты прав и репутации других лиц, охраны государственной безопасности, общественного порядка, здоровья или нравственности населения *(Правила поведения ШОС в области МИБ, A/69/723, п.7; Международный пакт о гражданских и политических правах, ст.19.2, Всеобщая декларация прав человека)*;

21. воздержание от любых клеветнических кампаний, оскорбительной или враждебной пропаганды с целью осуществления интервенции или вмешательства во внутренние дела других государств *(A/RES/73/27, PP20; A/RES/75/240, PP21).*

IV. Укрепление доверия и развитие сотрудничества в области обеспечения международной информационной безопасности

Следующие принципы и предложения могли бы лечь в основу положений Конвенции, регулирующих деятельность государств и определяющих их права и обязанности в части реализации задачи укрепления доверия и развития сотрудничества в области обеспечения международной информационной безопасности:

1. признание факта, что развитие международного сотрудничества по вопросам безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных

технологий будет способствовать повышению общего уровня безопасности, а также эффективности реагирования на соответствующие угрозы *(доклад РГОС 2021 г., A/75/816, п.3, 5; доклад ГПЭ 2021 г., A/76/135, п.5)*;

2. обмен национальным законодательством в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий и самих информационно-коммуникационных технологий *(промежуточный доклад РГОС 2022 г., A/77/275, раздел D, рекомендация 3; доклад ГПЭ 2021 г., A/76/135, п.83, 84)*;

3. оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации *(промежуточный доклад РГОС 2022 г., A/77/275, п.16 (c); доклад ГПЭ 2021 г., A/76/135, п.83; доклад ГПЭ 2015 г., A/70/174, п.13 (j))*;

4. оперативный обмен информацией о компьютерных инцидентах и совершенных в отношении государств компьютерных атаках с учетом того, что государствами может быть разработан стандартизированный набор технической информации, необходимой для передачи в целях реагирования на указанные угрозы *(доклад ГПЭ 2021 г., A/76/135, п.63)*;

5. проведение консультаций по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность, в целях предотвращения и мирного урегулирования конфликтов в информационном пространстве *(доклад ГПЭ 2021 г., A/76/135, п.23, 25)*;

6. развитие механизмов обмена передовым опытом реагирования на угрозы международной информационной безопасности *(доклад РГОС 2021 г., A/75/816, п.22, 43)*.

V. Содействие наращиванию потенциала государств в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий

Следующие принципы и предложения могли бы лечь в основу положений Конвенции, регулирующих деятельность государств и определяющих их права и обязанности в части реализации задачи содействия наращиванию потенциала государств в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий:

1. стимулирование взаимодействия между государствами в сфере обеспечения международной информационной безопасности для поддержания международного мира и безопасности *(доклад РГОС 2021 г., A/75/816, п.3)*;

2. содействие государствам в усилиях по наращиванию потенциала в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий по запросу каждого государства-реципиента и с учетом его потребностей и характеристик *(A/RES/77/36, PP5, OP6; A/RES/75/240, PP21; доклад РГОС 2021 г., A/75/816, п.56)*;

3. разработка под эгидой ООН универсальных принципов и программ оказания содействия развивающимся странам в наращивании их потенциала в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий *(доклад РГОС 2021 г., A/75/816, п.56)*;

4. развитие государственно-частного партнерства *(доклад РГОС 2021 г., A/75/816, п.18)*;

5. содействие разработке и использованию безопасных информационно-коммуникационных технологий с соблюдением принципа нейтральности глобальной сети связи, включая эволюционное реформирование протоколов и способов передачи информации для исключения возможности использования данной сети в противоправных целях;

6. недопустимость использования отдельными государствами и/или при их содействии частными компаниями технологического доминирования для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, включая основные информационные ресурсы, критическую инфраструктуру, ключевые технологии, продукты и услуги, а также для усиления технологической зависимости государств и препятствования осуществлению ими независимого контроля и проведению мероприятий, направленных на обеспечение информационной безопасности *(доклад РГОС 2021 г., A/75/816, п.11; вклад Китая в резюме председателя РГОС 2021 г., A/75/816*; *Правила поведения ШОС в области МИБ, A/69/723, п.5)*;

7. предотвращение дискриминации при осуществлении торгово-экономической деятельности с использованием информационно-коммуникационных технологий путем справедливого распределения доходов от нее, что способствовало бы укреплению национальных потенциалов государств в области обеспечения международной информационной безопасности *(доклад РГОС 2021 г., A/75/816, п.11; вклад Китая в резюме председателя РГОС 2021 г., A/75/816)*;

8. недопустимость злоупотреблений в отношении разработанных под контролем и юрисдикцией государств цепочек поставок в сфере информационно-коммуникационных технологий через создание факторов уязвимости продуктов, товаров и услуг в ущерб суверенитету и сохранности

данных отдельных государств (*доклад РГОС 2021 г., A/75/816, п.28; вклады Ирана, Китая в резюме председателя РГОС 2021 г., A/75/816)*;

9. недопустимость применения против государств неоправданных ограничений, в том числе односторонних принудительных мер, препятствующих всеобщему доступу к преимуществам от использования информационно-коммуникационных технологий в мирных целях, международному сотрудничеству или передаче таких технологий (*резюме председателя РГОС 2021 г., A/75/816, п.24; вклад Движения неприсоединения в резюме председателя РГОС 2021 г., A/75/816)*.

VI. Механизмы разработки и реализации конвенции

Проект будущей конвенции должен быть разработан под эгидой ООН при учете мнений всех государств-членов в рамках переговорного механизма, который должен быть создан для этих целей.

В соответствии с общепринятой практикой заключения многосторонних международных договоров будущая конвенция должна предусматривать механизмы контроля за выполнением государствами ее положений, внесения изменений и принятия дополнений, обмена мнениями по реализации документа, а также урегулирования и мирного разрешения споров. Механизм контроля за выполнением конвенции должен действовать под эгидой ООН при соблюдении принципов ее Устава, включая, прежде всего, суверенное равенство государств. Существующие примеры: постоянно действующие органы с участием всех государств, присоединившихся к конвенции, либо обзорные конференции, созываемые на регулярной основе. Конкретные параметры такого механизма должны быть определены в процессе согласования проекта конвенции.