СОГЛАШЕНИЕ
МЕЖДУ ПРАВИТЕЛЬСТВОМ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПРАВИТЕЛЬСТВОМ РЕСПУБЛИКИ ИНДИИ О СОТРУДНИЧЕСТВЕ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Правительство Российской Федерации и Правительство Республики Индии (далее именуемые "Стороны"),

учитывая развитие отношений между Российской Федерацией и Республикой Индией на основе взаимного доверия и сотрудничества,

отмечая значительный прогресс, достигнутый в развитии и внедрении новейших информационно-коммуникационных технологий (далее именуемых "ИКТ"),

признавая тот факт, что ИКТ по своему существу носят мирный характер и преследуют мирные цели, а также их значение для реализации потенциала развития стран с формирующейся экономикой и развивающихся стран,

выражая обеспокоенность по поводу угроз, связанных с возможностью использования таких технологий и средств коммуникации в целях, не совместимых с задачами обеспечения международной безопасности и стабильности как в гражданской, так и в военной сферах,

выражая обеспокоенность по поводу использования сохраняющихся "цифрового разрыва" и диспропорций в сфере ИКТ в ущерб интересам и безопасности других государств,

придавая большое значение безопасности в сфере использования ИКТ как одному из ключевых элементов системы международной безопасности,

будучи убеждены в том, что дальнейшее укрепление доверия и развитие взаимодействия Сторон в вопросах обеспечения безопасности

в сфере использования ИКТ являются настоятельной необходимостью и отвечают интересам Сторон,

принимая во внимание важную роль безопасности в сфере использования ИКТ в защите прав человека и основных свобод,

учитывая резолюции Генеральной Ассамблеи Организации Объединенных Наций "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности",

желая создать необходимые основы сотрудничества Сторон в вопросах обеспечения безопасности в сфере использования ИКТ,

согласились о нижеследующем:

Статья 1

Основные угрозы в области обеспечения безопасности в сфере использования ИКТ

Стороны осуществляют сотрудничество в соответствии с настоящим Соглашением, принимая во внимание наличие следующих основных угроз в области обеспечения безопасности в сфере использования ИКТ:

1) вредоносное использование ИКТ, направленное на подрыв суверенитета, нарушение территориальной целостности и создание угрозы международному миру, правам человека, свободе выражения мнений, безопасности и стратегической стабильности;

2) вредоносные атаки на критическую информационную инфраструктуру, которые могут подорвать безопасное и стабильное функционирование глобальных и национальных информационно-коммуникационных сетей, в том числе действия, способные нанести экономический вред;

3) террористические акты, в том числе пропаганда терроризма и вербовка для осуществления террористической деятельности, совершаемой с использованием ИКТ;

4) преступные деяния, совершаемые с использованием ИКТ;

5) распространение информации с использованием ИКТ с целью нарушить общественный порядок, общинное и социальное согласие и подорвать осуществление государственного управления;

6) угрозы безопасному и стабильному функционированию глобальной и национальной информационной инфраструктуры, имеющие природный и (или) техногенный характер.

Статья 2

Основные направления сотрудничества

С учетом угроз, указанных в статье 1 настоящего Соглашения, Стороны, их уполномоченные представители, а также компетентные органы государств Сторон, которые определяются в соответствии со статьей 4 настоящего Соглашения, осуществляют сотрудничество в области обеспечения безопасности в сфере использования ИКТ по следующим основным направлениям:

1) определение, координация и осуществление необходимых мер по обеспечению безопасности в сфере использования ИКТ;

2) создание системы защищенного обмена информацией, которой располагают Стороны, о подобных нападениях, об их источниках, исполнителях и о снижении последствий инцидентов и нападений с использованием ИКТ;

3) содействие выработке мер в области ограничения распространения и использования вредоносных средств и уязвимостей в сфере использования ИКТ, которые могут угрожать национальной и общественной безопасности, в том числе на международном уровне;

4) противодействие угрозам использования ИКТ в террористических целях;

5) противодействие использованию ИКТ в преступных целях, в том числе путем содействия сотрудничеству между правоохранительными органами государств Сторон посредством приближенного к реальному времени обмена информацией и сбора доказательств;

6) создание механизма двустороннего сотрудничества в области исследований и развития, в том числе в сфере технологий, стандартов, методов проведения испытаний и разработки средств для обеспечения безопасности в сфере использования ИКТ;

7) повышение транспарентности, подотчетности и инклюзивности в области управления глобальной сетью Интернет и поддержание ее безопасности и стабильного функционирования;

8) разработка совместных мер по обеспечению безопасности критической инфраструктуры государств Сторон, обозначенной ими;

9) укрепление мер доверия, способствующих обеспечению безопасности в сфере использования ИКТ;

10) обмен информацией о политике и об организационно-технических процедурах по использованию электронной подписи и защите информации при международном информационном обмене;

11) обмен информацией о национальных стратегиях и соответствующем законодательстве каждого из государств Сторон по вопросам обеспечения безопасности в сфере использования ИКТ;

12) содействие совершенствованию международно-правовых рамок и практических механизмов сотрудничества Сторон в области обеспечения безопасности в сфере использования ИКТ;

13) создание условий для взаимодействия компетентных органов государств Сторон в целях реализации настоящего Соглашения;

14) тесное взаимодействие и сотрудничество в рамках международных организаций и форумов по проблемам обеспечения безопасности в сфере использования ИКТ;

15) обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других мероприятий с участием уполномоченных представителей и экспертов Сторон в области обеспечения безопасности в сфере использования ИКТ;

16) сотрудничество в области наращивания потенциала и наработки навыков в области обеспечения безопасности в сфере использования ИКТ, борьбы с преступлениями, совершаемыми с использованием ИКТ, и в области проведения криминалистических исследований, связанных с ИКТ;

17) развитие сотрудничества в сфере обмена информацией между соответствующими уполномоченными органами государств Сторон в области выявления, предотвращения и снижения последствий компьютерных атак (группа реагирования на компьютерные чрезвычайные ситуации/команда по реагированию на инциденты в области компьютерной безопасности);

18) обмен информацией по вопросам, связанным с осуществлением сотрудничества по указанным в настоящей статье основным направлениям.

Стороны и компетентные органы государств Сторон могут по взаимной договоренности определять другие направления сотрудничества.

Статья 3

Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество и деятельность в рамках настоящего Соглашения таким образом, чтобы такая

деятельность способствовала социальному и экономическому развитию и была совместимой с задачами поддержания международного мира, безопасности и стабильности и соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения основных свобод, а также принципам двустороннего сотрудничества и невмешательства в информационные ресурсы государств Сторон.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с правом каждой Стороны искать, получать и распространять информацию с учетом того, что такое право может быть ограничено законодательством государств Сторон в целях обеспечения национальной безопасности.

3. Каждая Сторона имеет равные права на защиту своей соответствующей информационно-коммуникационной инфраструктуры, информации, проходящей через такую инфраструктуру и критические структуры, такие как правительственные объекты, системы и учреждения, нарушение работы которых может нанести серьезный ущерб национальной безопасности государства, от неправомерного использования и вмешательства, включая нападения на них с использованием ИКТ.

Статья 4

Механизмы сотрудничества

1. Стороны содействуют налаживанию Совместного диалога между заместителем Секретаря Совета Безопасности Российской Федерации и заместителем Советника по вопросам национальной безопасности Республики Индии в качестве основного механизма для определения направлений в основных сферах сотрудничества

и совместного обзора осуществления мероприятий, согласованных в рамках настоящего Соглашения.

2. В течение шестидесяти дней с даты вступления настоящего Соглашения в силу Стороны обмениваются по дипломатическим каналам данными о соответствующих компетентных органах государств Сторон, ответственных за выполнение настоящего Соглашения, и каналах прямого обмена информацией по конкретным направлениям сотрудничества.

3. С целью рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и оценки связанных с ИКТ угроз, а также определения, согласования и координации мер реагирования Стороны проводят на регулярной основе консультации уполномоченных представителей Сторон и соответствующих компетентных органов государств Сторон (далее – консультации).

Очередные консультации проводятся по согласованию Сторон, как правило, в Российской Федерации и Республике Индии на ротационной основе.

Любая из Сторон может инициировать проведение дополнительных консультаций, предложив время и место их проведения, а также повестку дня.

4. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии соответствующих компетентных органов государств Сторон, ответственных за выполнение настоящего Соглашения.

5. В целях создания необходимой институциональной базы сотрудничества по конкретным направлениям соответствующие компетентные органы государств Сторон могут заключать надлежащие договоры межведомственного характера.

Статья 5

Конфиденциальность информации

1. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, доступной для официального использования исключительно для целей настоящего Соглашения.

2. Защита такой информации осуществляется в соответствии с законодательством государства получающей Стороны, а также двусторонними соглашениями между Сторонами по аналогичным вопросам. Такая информация не раскрывается и не передается третьим сторонам без письменного согласия Стороны, являющейся источником этой информации.

Статья 6

Финансирование

1. Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.

2. В отношении прочих расходов, связанных с исполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с законодательством каждого из государств Сторон.

Статья 7

Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участниками которых являются государства.

Статья 8

Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров между компетентными органами государств Сторон и, в случае необходимости, по дипломатическим каналам.

Статья 9

Рабочие языки

Рабочими языками при осуществлении сотрудничества в рамках настоящего Соглашения являются русский и английский языки.

Статья 10

Заключительные положения

1. Настоящее Соглашение вступает в силу на тридцатый день с даты получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу. Оно действует в течение пяти лет и автоматически продлевается на последующие пятилетние периоды.

2. По взаимному согласию Стороны могут вносить изменения в настоящее Соглашение, которые оформляются отдельным протоколом.

3. Каждая из Сторон может прекратить действие настоящего Соглашения путем направления другой Стороне по дипломатическим каналам письменного уведомления о таком решении. В этом случае действие настоящего Соглашения прекращается по истечении девяноста дней после получения такого уведомления.

4. В случае прекращения действия настоящего Соглашения Стороны принимают меры для полного выполнения обязательств по защите информации, а также ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках Соглашения и не завершенных к моменту прекращения действия Соглашения.

В удостоверение чего нижеподписавшиеся представители, должным образом уполномоченные на это своими правительствами, подписали настоящее Соглашение.

Совершено в Гоа «15» октября 2016 года в двух экземплярах на русском, хинди и английском языках, причем все тексты имеют одинаковую силу.

За Правительство Российской Федерации

За Правительство Республики Индии