СОГЛАШЕНИЕ

между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности

Правительство Российской Федерации и Правительство Исламской Республики Иран, далее именуемые Сторонами,

ссылаясь на Договор об основах взаимоотношений и принципах сотрудничества между Российской Федерацией и Исламской Республикой Иран от 12 марта 2001 г.,

отмечая значительный прогресс, достигнутый в развитии и внедрении новейших информационно-коммуникационных технологий,

отмечая большое значение информационно-коммуникационных технологий для социально-экономического развития на благо всего человечества, а также для поддержания в современных условиях международного мира, безопасности и стабильности,

выражая озабоченность по поводу угроз, связанных с возможностями использования таких технологий в целях, несовместимых с задачами обеспечения международного мира, безопасности и стабильности, для подрыва суверенитета и безопасности государств и вмешательства в их внутренние дела, нарушения неприкосновенности частной жизни граждан, дестабилизации внутриполитической и социально-экономической обстановки, разжигания межнациональной и межрелигиозной вражды,

подчеркивая необходимость получения максимальной отдачи от информационно-коммуникационных технологий и уменьшения исходящих от них в свой адрес общих угроз,

подчеркивая также настоятельную потребность соблюдения законов и правил государств Сторон в выполнении настоящего Соглашения,

признавая растущее значение информационной безопасности для системы международной безопасности,

подтверждая, что государственный суверенитет и международные нормы и принципы, вытекающие из государственного суверенитета, распространяются на поведение государств в рамках деятельности, связанной с использованием информационно-коммуникационных технологий, и их юрисдикцию над информационно-коммуникационной инфраструктурой на их территории, а также подтверждая то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью "Интернет", включая обеспечение безопасности,

будучи убеждены в том, что дальнейшее укрепление доверия и развитие взаимодействия между Сторонами в области использования информационно-коммуникационных технологий являются настоятельной необходимостью и отвечают их интересам,

придавая важное значение балансу между обеспечением безопасности и соблюдением прав человека в области использования информационно-коммуникационных технологий в соответствии с национальным законодательством, а также международными обязательствами государств Сторон,

стремясь предотвращать угрозы информационной безопасности и бороться с ними, обеспечивать интересы государств Сторон в области обеспечения информационной безопасности в целях формирования мирной и безопасной международной информационной среды,

осуждая односторонние принудительные меры, принимаемые в нарушение Устава Организации Объединенных Наций,

стремясь к дальнейшей совместной работе в целях уменьшения уязвимости государств перед лицом возникающих угроз информационной

безопасности, включая угрозу принятия в отношении государств Сторон мер по ограничению или блокировке использования ИКТ и доступа в Интернет,

стремясь также к тесному сотрудничеству на региональных и международных форумах в целях разработки и продвижения правовых норм и правил для обеспечения международной информационной безопасности, в том числе путем справедливого управления Интернетом,

желая создать общие основы сотрудничества государств Сторон в области обеспечения информационной безопасности,

договорились о нижеследующем:

Статья 1
Основные термины

1. Для целей выполнения настоящего Соглашения Стороны согласовывают определения основных терминов, которые приведены в приложении, являющемся неотъемлемой частью настоящего Соглашения.

2. В приложение по мере необходимости могут вноситься изменения и обновления по согласованию Сторон.

Статья 2
Основные угрозы
в области обеспечения информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами в области обеспечения информационной безопасности является использование информационно-коммуникационных технологий:

1) для осуществления актов, направленных на нарушение суверенитета, безопасности и территориальной целостности государств;

2) для нанесения экономического и другого ущерба, в том числе путем разрушительного воздействия на объекты критической информационной и другой соответствующей информационной инфраструктуры;

3) в террористических целях, в том числе для пропаганды терроризма и вербовки для осуществления террористической деятельности;

4) для совершения преступлений, в том числе связанных с несанкционированным доступом к компьютерной информации;

5) для вмешательства во внутренние дела государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межрелигиозной вражды, распространения расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической и социально-экономической обстановки и вмешательства в государственное управление;

6) для распространения информации, наносящей вред общественно-политической и социально-экономической системам, а также духовной, нравственной и культурной среде других государств.

Статья 3

Основные направления двустороннего сотрудничества

1. С учетом основных угроз, указанных в статье 2 настоящего Соглашения, и необходимости обеспечивать информационную безопасность Стороны, уполномоченные представители и компетентные органы государств Сторон, которые определяются в соответствии

со статьей 5 настоящего Соглашения, будут осуществлять сотрудничество по таким вопросам, как укрепление информационной безопасности, борьба с преступлениями, связанными с использованием информационно-коммуникационных технологий, оказание технической и технологической помощи, а также международное взаимодействие, в частности, по следующим основным направлениям:

1) определение, согласование и осуществление необходимого взаимодействия в рамках региональных и международных форумов для обеспечения национальной и международной информационной безопасности;

2) разработка и продвижение норм применимого международного права в целях обеспечения национальной и международной информационной безопасности;

3) противодействие угрозам в области обеспечения информационной безопасности, указанным в статье 2 настоящего Соглашения;

4) обмен информацией и взаимодействие в правоохранительной области в целях предупреждения, выявления, пресечения и расследования преступлений, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях, а также уголовного преследования за такие преступления;

5) участие в многосторонних переговорах по мерам укрепления доверия, связанных с обеспечением международной информационной безопасности;

6) обмен информацией между компетентными органами государств Сторон в области информационной безопасности, включая сотрудничество между уполномоченными органами государств Сторон в области реагирования на компьютерные инциденты;

7) обмен информацией о законодательстве государств Сторон по вопросам обеспечения информационной безопасности;

8) сотрудничество в целях устранения негативных последствий односторонних принудительных мер, принимаемых в нарушение Устава Организации Объединенных Наций и международного права, в области обеспечения информационной безопасности;

9) содействие совершенствованию двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в обеспечении национальной и международной информационной безопасности;

10) создание условий для взаимодействия компетентных органов государств Сторон по указанным в статье 3 настоящего Соглашения основным направлениям сотрудничества, а также по другим возможным направлениям в целях реализации настоящего Соглашения;

11) углубление взаимодействия и координации деятельности государств Сторон в области международной информационной безопасности в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Международную организацию по стандартизации, Интерпол, Шанхайскую организацию сотрудничества и другие соответствующие региональные и международные организации);

12) оказание содействия в соответствии с законодательством государств Сторон в области передачи информационных технологий и знаний, наращивания потенциала и развития профессиональной подготовки, а также изучение возможностей инвестирования в инфраструктуры информационной безопасности;

13) способствование взаимодействию научных и образовательных учреждений, а также частных секторов в области информационной безопасности;

14) проведение двусторонних рабочих встреч, конференций, семинаров и форумов по вопросам, касающимся обозначенных

направлений сотрудничества, а также совместная организация и проведение мероприятий на региональном и международном уровнях в сфере национальной и международной информационной безопасности.

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

Статья 4

Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения национальной и международной информационной безопасности в рамках настоящего Соглашения таким образом, чтобы такое сотрудничество способствовало социальному и экономическому развитию, было совместимо с задачами поддержания международного мира, безопасности и стабильности и соответствовало их национальным законам и нормативным актам, а также общепризнанным принципам и нормам международного права, включая принципы взаимного уважения суверенитета и территориальной целостности, мирного урегулирования споров и конфликтов, неприменения силы и угрозы силой, невмешательства во внутренние дела, уважения прав человека и 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 информационных ресурсов своего государства от неправомерного использования

и несанкционированного вмешательства, в том числе от компьютерных атак на них. Каждая Сторона не осуществляет по отношению к другой Стороне подобных действий и оказывает содействие другой Стороне в реализации указанных прав.

Статья 5

Основные формы и механизмы сотрудничества

1. Стороны определят компетентные органы государств Сторон, ответственные за реализацию настоящего Соглашения, и в течение 60 дней со дня вступления настоящего Соглашения в силу назначат и обменяются по дипломатическим каналам данными об указанных компетентных органах государств Сторон.

2. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям сотрудничества в соответствии с настоящим Соглашением компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

3. В целях контроля за выполнением настоящего Соглашения, рассмотрения вопросов, возникающих в ходе его реализации, обмена информацией, анализа и совместной оценки возникающих угроз международной информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы Стороны проводят заседания в рамках механизма регулярных консультаций с участием уполномоченных представителей и компетентных органов не реже одного раза в год попеременно в Российской Федерации и Исламской Республике Иран.

Статья 6

Защита информации

1. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в рамках настоящего Соглашения информации, доступ к которой ограничен в соответствии с законодательством государств Сторон.

2. Каждая из Сторон не раскрывает и не передает третьей стороне без предварительного письменного согласия другой Стороны информацию, полученную или совместно созданную в контексте реализации настоящего Соглашения.

3. Необходимость сохранения в тайне информации, касающейся отдельных аспектов сотрудничества между Сторонами, или иных данных заблаговременно доводится одной Стороной до сведения другой Стороны.

4. Любая информация, передаваемая в рамках настоящего Соглашения, используется исключительно в целях настоящего Соглашения. Информация, полученная одной из Сторон, не должна использоваться в ущерб другой Стороне.

5. Любая информация, имеющая ограничения по доступу, защищается в соответствии с законодательством государств Сторон.

6. Порядок передачи и защиты секретной информации определяется Соглашением между Правительством Российской Федерации и Правительством Исламской Республики Иран о взаимной защите секретной информации от 6 февраля 2008 г.

Статья 7

Финансирование

1. Стороны самостоятельно несут расходы, связанные с участием их представителей и экспертов в соответствующих мероприятиях по выполнению настоящего Соглашения.

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

Статья 8

Разрешение споров

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

Статья 9

Заключительные положения

1. Настоящее Соглашение вступает в силу на 30-й день со дня получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

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

3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней со дня получения одной из Сторон по дипломатическим каналам письменного уведомления другой Стороны о ее намерении прекратить действие настоящего Соглашения.

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

Совершено в г. Москве "26" января 2021 г. в двух экземплярах, каждый на русском, персидском и английском языках, причем все тексты имеют одинаковую силу. В случае расхождений будет использоваться текст на английском языке.

За Правительство Российской Федерации

За Правительство Исламской Республики Иран

ПРИЛОЖЕНИЕ
к Соглашению между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности

ОСНОВНЫЕ ПОНЯТИЯ,

приведенные в Соглашении между Правительством Российской Федерации и Правительством Исламской Республики Иран о сотрудничестве в области обеспечения информационной безопасности

1. **"Информационная безопасность"** - состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве.

2. **"Международная информационная безопасность"** - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

3. **"Информационное пространство"** - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием и хранением информации, оказывающая воздействие, в частности, на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию.

4. **"Угрозы информационной безопасности"** - совокупность действий и факторов, создающих опасность нанесения вреда информационной безопасности.

5. **"Информационная инфраструктура"** - ряд технических средств и систем для формирования, создания, преобразования, передачи, использования и хранения информации.

6. **"Объекты критической информационной инфраструктуры"** - информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления, определенные в соответствии с законодательством государств Сторон.

7. **"Компьютерный инцидент"** - факт нарушения и (или) прекращения функционирования объекта информационной инфраструктуры, сети электросвязи, используемой для организации взаимодействия таких объектов, и (или) нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки.

8. **"Компьютерная атака"** - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.