СОГЛАШЕНИЕ
между Правительством Российской Федерации и Правительством Республики Куба о сотрудничестве в области обеспечения международной информационной безопасности

Правительство Российской Федерации и Правительство Республики Куба, далее именуемые Сторонами,

отмечая значительный прогресс в развитии и внедрении новейших информационных и коммуникационных технологий и средств, формирующих глобальное информационное пространство,

выражая озабоченность угрозами, связанными с возможностями использования в гражданской и военной сферах таких технологий и средств в целях, не совместимых с задачами обеспечения международного мира, безопасности и стабильности,

придавая важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности,

будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон по вопросам обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,

ставя цель обеспечивать безопасность и интересы государств Сторон в информационном пространстве,

принимая во внимание важную роль информационной безопасности в обеспечении прав и основных свобод человека и гражданина,

учитывая ежегодные резолюции Генеральной Ассамблеи ООН «Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности»,

стремясь ограничить угрозы международной информационной безопасности, обеспечить интересы информационной безопасности Сторон и

внести вклад в формирование международной информационной среды, для которой характерны мир, сотрудничество и гармония,

признавая, что незаконное использование информационных и коммуникационных технологий лицами, организациями и государствами в ущерб другим государствам вызывает серьезную озабоченность, поскольку потенциально может способствовать возникновению международных конфликтов,

будучи убежденными в том, что сотрудничество Сторон является действенным механизмом предотвращения рисков, угроз и агрессии, противостояния им, а также недопущения превращения информационного пространства в театр военных действий,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности,

согласились о нижеследующем:

Статья 1
Основные понятия

Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, перечень которых приведен в приложении, являющемся неотъемлемой частью настоящего Соглашения.

Статья 2
Основные угрозы в области обеспечения международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами международной информационной безопасности является неправомерное использование информационных и коммуникационных технологий:

1) в качестве информационного оружия в военно-политических целях, противоречащих международному праву, для осуществления враждебных

действий и актов агрессии, направленных на нарушение суверенитета, территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности;

2) в террористических целях, в том числе для оказания деструктивного воздействия на критическую информационную инфраструктуру, а также для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

3) для вмешательства во внутренние дела суверенных государств, нарушения общественного порядка, разжигания межнациональной, межрасовой и межконфессиональной вражды, пропаганды расистских и ксенофобских идей и теорий, порождающих ненависть и дискриминацию, подстрекающих к насилию и нестабильности, а также для дестабилизации внутриполитической обстановки, нарушения управления государством и в целях свержения конституционного строя;

4) для совершения преступлений, в том числе связанных с неправомерным доступом к информационным ресурсам, с созданием, использованием и распространением вредоносных компьютерных программ;

5) для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств;

6) для нанесения ущерба третьим странам с использованием информационного пространства и информационных ресурсов государств Сторон.

Статья 3
Основные направления сотрудничества

С учетом основных угроз, указанных в статье 2 настоящего Соглашения, Стороны, их уполномоченные представители, а также компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют

сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) определение, согласование и осуществление необходимых совместных мер в области обеспечения международной информационной безопасности;

2) создание механизмов двустороннего сотрудничества в целях предотвращения угроз информационной безопасности и противодействия им;

3) создание системы мониторинга и совместного реагирования на возникающие в этой области угрозы;

4) выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы национальной безопасности, а также международному миру и безопасности;

5) противодействие указанным в статье 2 настоящего Соглашения угрозам использования информационных и коммуникационных технологий;

6) проведение экспертиз, исследований и оценок в области обеспечения информационной безопасности;

7) содействие обеспечению безопасного, стабильного функционирования и интернационализации управления информационно-телекоммуникационной сетью «Интернет»;

8) обеспечение информационной безопасности критически важных объектов государств Сторон;

9) разработка и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности;

10) разработка и осуществление согласованной политики по защите информации, в том числе защите персональных данных, при трансграничном информационном взаимодействии;

11) обмен информацией о законодательстве государства каждой из Сторон по вопросам обеспечения информационной безопасности;

12) содействие совершенствованию международно-правовой базы и практических механизмов сотрудничества Сторон в обеспечении международной информационной безопасности;

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

14) взаимодействие в рамках международных организаций и форумов по проблемам обеспечения международной информационной безопасности;

15) содействие обмену оборудованием, технологиями и специализированными системами для повышения потенциала государств Сторон по предотвращению угроз информационной безопасности и противодействию этим угрозам;

16) наращивание обмена опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов Сторон в области информационной безопасности;

17) обмен информацией по основным направлениям сотрудничества, перечисленным в настоящей статье, в том числе с использованием каналов прямой связи между государствами Сторон.

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 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 общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов,

неприменения силы и угрозы силой, невмешательства во внутренние дела, уважения прав и свобод человека, 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 государства каждой Стороны в целях обеспечения национальной безопасности.

3. Каждая Сторона имеет равное право на защиту информационных ресурсов своего государства от действий по неправомерному использованию и несанкционированному вмешательству, 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 указанного права.

Статья 5
Основные формы и механизмы сотрудничества

1. В течение 60 дней с даты вступления настоящего Соглашения в силу Стороны обменяются по дипломатическим каналам сведениями о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения.

2. С целью рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы Стороны проводят на регулярной основе консультации уполномоченных представителей Сторон и компетентных органов государств Сторон (далее - консультации).

Консультации проводятся по согласованию Сторон, как правило, 2 раза в год, попеременно в Российской Федерации и в Республике Куба.

Каждая из Сторон может инициировать проведение дополнительных консультаций, предлагая их время и место, а также повестку дня.

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

4. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы государств Сторон могут заключать соответствующие договоры межведомственного характера.

Статья 6
Защита информации

Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, доступ к которой и распространение которой ограничены в соответствии с законодательством государства каждой из Сторон.

Защита такой информации осуществляется в соответствии с законодательством государства получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия Стороны, передавшей эту информацию.

Такая информация должным образом обозначается в соответствии с законодательством государств Сторон. Защита государственной тайны Российской Федерации и (или) государственной тайны Республики Куба в ходе сотрудничества в рамках настоящего Соглашения осуществляется в соответствии с Соглашением между Правительством Российской Федерации и Правительством Республики Куба о взаимной защите секретной

информации от 22 октября 2010 г., а также законодательством государства каждой из Сторон.

Статья 7
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 своих государств.

Статья 8
Отношение к другим международным договорам

Стороны осуществляют сотрудничество в соответствии с законодательствами своих государств, а также общепризнанными нормами и принципами международного права.

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство.

Статья 9
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 и, в случае необходимости, по дипломатическим каналам.

Статья 10
Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на 30-й день с даты получения по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

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

3. Действие настоящего Соглашения может быть прекращено по истечении 90 дней с даты 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. Гаване «11» мая 2014 г. в двух экземплярах на русском и испанском языках, причем оба текста имеют одинаковую силу.

За Правительство Российской Федерации	**За Правительство Республики Куба**

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

ПЕРЕЧЕНЬ
основных понятий, используемых для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения

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

«Информационная война» - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны.

«Информационная инфраструктура» - совокупность технических средств и систем создания, преобразования, передачи, использования и хранения информации.

«Информационное оружие» - информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

«Информационное пространство» - сфера деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и

общественное сознание, информационную инфраструктуру и собственно информацию.

«Информационные ресурсы» - информационная инфраструктура, а также собственно информация и ее потоки.

«Защита информации» - комплекс правовых, организационных и технических мер, направленных на обеспечение целостности (неизменности), конфиденциальности, доступности и сохранности информации.

«Критически важные объекты» - объекты инфраструктуры государства, нарушение или прекращение функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению или разрушению экономики государства либо административно-территориальной единицы или существенному ухудшению безопасности жизнедеятельности населения, проживающего на территории государства, на длительный срок.

«Международная информационная безопасность» - такое состояние глобального информационного пространства, при котором исключены возможности нарушения прав личности, общества и прав государства в информационной сфере, а также деструктивного и противоправного воздействия на критическую информационную инфраструктуру.

«Неправомерное использование информационных ресурсов» - использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств каждой из Сторон либо норм международного права.

«Несанкционированное вмешательство в информационные ресурсы» - неправомерное воздействие на процессы создания, обработки, преобразования, передачи, использования, хранения информации.

«Угроза информационной безопасности» - факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.