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

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

руководствуясь Договором о создании Союзного государства от 8 декабря 1999 года,

отмечая значительный прогресс в развитии и внедрении новейших информационно-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 международной 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,

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

учитывая 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,

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 № 1, 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 наличия следующих основных угроз в области обеспечения международной информационной безопасности:

1) разработка и применение информационного оружия, подготовка и ведение информационной войны;

2) информационный терроризм;

3) информационная преступность;

4) использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств;

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

6) угрозы безопасному и стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Согласованное понимание Сторонами существа указанных основных угроз отражено в перечне основных угроз в области международной информационной безопасности, их источников и признаков, предусмотренном Приложением № 2, являющемся неотъемлемой частью настоящего Соглашения.

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

3) выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, национальной и общественной безопасности;

4) противодействие угрозам использования информационно-коммуникационных технологий в террористических целях;

5) противодействие информационной преступности;

6) проведение необходимых для целей настоящего Соглашения экспертиз, исследований и оценок в области обеспечения информационной безопасности;

7) содействие обеспечению безопасного, стабильного функционирования и интернационализации управления 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 использованию электронной подписи (электронной цифровой подписи) и защите информации, в том числе защите персональных данных, при трансграничном информационном взаимодействии;

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

12) совершенствование 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) обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов Сторон в области информационной безопасности;

16) обмен информацией по вопросам, связанным с осуществлением сотрудничества по перечисленным в настоящей статье основным направлениям;

17) формирование и осуществление согласованной в рамках Союзного государства военной политики в области международной информационной безопасности.

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

Статья 4
Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество и свою деятельность в международном информационном пространстве в рамках настоящего Соглашения таким образом, чтобы как сотрудничество, так и деятельность способствовали социальному и экономическому развитию, были совместимы с задачами поддержания международной безопасности и стабильности и соответствовали общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных 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 защиты интересов национальной и общественной безопасности.

3. Каждая Сторона имеет равное право на защиту информационных ресурсов и критически важных объектов своего государства от

неправомерного использования и несанкционированного вмешательства, в том числе от информационных 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 данными 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).

Очередные консультации проводятся по согласованию Сторон, как правило 2 раза в год, попеременно в Республике Беларусь и Российской Федерации.

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) государственных секретов Республики Беларусь в ходе сотрудничества в рамках настоящего Соглашения осуществляется в соответствии с Соглашением между Российской Федерацией и Республикой Беларусь о взаимном обеспечении защиты государственной тайны Российской Федерации и государственных секретов Республики Беларусь от 20 января 2003 года, а также законодательством государств 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

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 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 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 городе Москве 25 декабря 2013 года в двух экземплярах на русском языке.

За Правительство Российской Федерации

За Правительство Республики Беларусь

ПРИЛОЖЕНИЕ № 1
к Соглашению между Правительством
Российской Федерации и
Правительством Республики Беларусь
о сотрудничестве в области
обеспечения международной
информационной безопасности

ПЕРЕЧЕНЬ
основных понятий в области обеспечения
международной информационной безопасности

«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.

«Информационная преступность» - использование информационных ресурсов и (или) воздействие на них в информационном пространстве

в противоправных целях.

«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.

«Информационный терроризм» - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях.

«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 этих территориях, на длительный срок.

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

«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.

ПРИЛОЖЕНИЕ № 2
к Соглашению между Правительством
Российской Федерации и
Правительством Республики Беларусь
о сотрудничестве в области
обеспечения международной
информационной безопасности

ПЕРЕЧЕНЬ
основных угроз в области международной информационной безопасности, их источников и признаков

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

Источник угрозы - создание и развитие информационного оружия, способного нанести ущерб критически важным объектам государств, что может привести к новой гонке вооружений.

Признаки угрозы - применение информационного оружия в целях подготовки и ведения информационной войны, воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах; деструктивное воздействие на критически важные объекты.

2. Информационный терроризм.

Источник угрозы - террористические организации и лица, причастные к террористической деятельности, осуществляющие

противоправные действия посредством или в отношении информационных ресурсов.

Признаки угрозы - использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящее к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование сети «Интернет» или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе; иное негативное воздействие на информационные ресурсы.

3. Информационная преступность.

Источник угрозы - лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Признаки угрозы - проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление сетевых атак и иного негативного воздействия; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т.д.

4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других государств.

Источник угрозы - неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению «цифрового разрыва» между развитыми и развивающимися странами. Некоторые государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие других стран и получение доступа к информационным технологиям, что приводит к возникновению серьезной опасности для государств с недостаточными информационными возможностями.

Признаки угрозы - монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств; встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемые в другие страны, для контроля и влияния на информационные ресурсы и (или) критически важные объекты этих стран; контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств.

5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Источники угрозы - государства, организации, группа лиц или частные лица, использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Признаки угрозы - появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в сети «Интернет» и других сетях информационного обмена информации:

искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;

пропагандирующей идеи терроризма, сепаратизма и экстремизма;

разжигающей межнациональную, межрасовую и межконфессиональную вражду.

6. Угрозы безопасному и стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и (или) техногенный характер.

Источники угроз - стихийные бедствия и другие опасные природные явления, а также катастрофы техногенного характера, способные оказать масштабное разрушительное воздействие на информационные ресурсы государства.

Признаки угроз - нарушение функционирования объектов информационной инфраструктуры и, следовательно, дестабилизация критически важных объектов, государственных систем управления и принятия решений, результаты которой прямо затрагивают безопасность государства и общества.