



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 28 декабря 2018 г. № 2984-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Индонезии о сотрудничестве в области обеспечения международной информационной безопасности

В соответствии с пунктом 1 статьи 11 Федерального закона "О международных договорах Российской Федерации" одобрить представленный МИДом России согласованный с другими заинтересованными федеральными органами исполнительной власти и аппаратом Совета Безопасности Российской Федерации и предварительно проработанный с Индонезийской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Республики Индонезии о сотрудничестве в области обеспечения международной информационной безопасности (прилагается).

Поручить МИДу России провести переговоры с Индонезийской Стороной и по достижении договоренности подписать от имени Правительства Российской Федерации указанное Соглашение, разрешив вносить в прилагаемый проект изменения, не имеющие принципиального характера.

Председатель Правительства
Российской Федерации



Д.Медведев

СОГЛАШЕНИЕ

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

Правительство Российской Федерации и Правительство Республики Индонезии, 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 меры укрепления доверия будут способствовать дальнейшему углублению взаимного доверия и развитию взаимодействия Сторон по вопросам обеспечения международной информационной безопасности, что является настоятельной необходимостью и отвечает их интересам,

ставя цель обеспечивать безопасность и интересы государств Сторон в информационном пространстве на двустороннем, региональном, международном уровнях,

отмечая важность уважения прав и основных свобод человека в сфере использования информационных и коммуникационных технологий;

ссылаясь на 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 Российской Федерации и Республики Индонезии 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 может вызвать международные напряженности и конфликты,

будучи убежденными в том, что эффективное и действенное сотрудничество Сторон является основой для предотвращения рисков и противостояния угрозам, а также недопущения использования информационного пространства в военных целях,

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

согласились о нижеследующем:

Статья 1

Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения международной информационной безопасности в целях поддержания международного мира, безопасности и стабильности, которое соответствует общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров, неприменения силы и угрозы применения силы против территориальной целостности Российской Федерации и Республики Индонезии, невмешательства во внутренние дела суверенных государств, уважения основных прав и свобод человека, а также невмешательства в информационные ресурсы Российской Федерации и Республики Индонезии.

2. Каждая Сторона имеет равное право на защиту соответствующих информационных ресурсов своего государства от действий по неправомерному использованию и несанкционированному вмешательству, в том числе от компьютерных атак на них.

3. Стороны укрепляют взаимное доверие в рамках настоящего Соглашения и не предпринимают какие-либо действия, указанные в статье 3 настоящего Соглашения, против другой Стороны, а также оказывают помощь другой Стороне при поступлении соответствующей просьбы в целях осуществления ранее упомянутых прав.

Статья 2

Направления сотрудничества

Стороны ведут сотрудничество по следующим направлениям:

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

2) создание практических механизмов конкретного двустороннего сотрудничества в целях предотвращения и устранения угроз информационной безопасности;

3) создание системы предотвращения, мониторинга и совместного реагирования на возникающие в области обеспечения международной информационной безопасности угрозы;

4) обмен информацией о противоправном использовании информационных и коммуникационных технологий, компьютерных инцидентах, вредоносном программном обеспечении, компьютерных атаках и иных способах противоправного использования информационных и коммуникационных технологий, которое представляет угрозу безопасности Российской Федерации и Республики Индонезии;

5) содействие обеспечению безопасного и стабильного функционирования и интернационализации управления информационно-телекоммуникационной сетью "Интернет"(далее - сеть "Интернет");

6) взаимодействие Сторон по совершенствованию действующей модели управления сетью "Интернет", в том числе обеспечению равного права государств на участие в процессе управления сетью "Интернет" и повышения в этом контексте роли Международного союза электросвязи;

7) разработка и осуществление совместных мер доверия в области использования информационных и коммуникационных технологий, способствующих обеспечению международной информационной безопасности;

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

9) обмен информацией о национальном законодательстве по вопросам обеспечения информационной безопасности;

10) содействие развитию международно-правовой базы по вопросам международной информационной безопасности и созданию норм и принципов ответственного поведения государств, а также формирование общего понимания того, как международное право применяется государствами в сфере использования информационных

и коммуникационных технологий, в том числе в случае их вредоносного использования;

11) создание условий для эффективного взаимодействия компетентных органов Российской Федерации и Республики Индонезии в целях реализации настоящего Соглашения;

12) сотрудничество и координация действий в рамках соответствующих международных организаций и форумов по обеспечению достижения общих целей в области международной информационной безопасности;

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

14) совместные меры, включающие расследование, отслеживание и обнаружение, по предотвращению и устранению угроз, указанных в статье 3 настоящего соглашения, и противоправного использования информационных и коммуникационных технологий, исходящих от граждан, организаций или государств, которые потенциально способны подвергнуть опасности территории и безопасность Российской Федерации и Республики Индонезии;

15) выработка совместных мер по развитию анализа вредоносного программного обеспечения, лабораторий по его исследованию, а также испытательных лабораторий, связанных с программным обеспечением и оборудованием, предназначенными для обеспечения информационной безопасности;

16) обмен взглядами на концепцию защиты критической информационной инфраструктуры Российской Федерации и Республики Индонезии;

17) содействие обнаружению инцидентов и моделированию реагирования на угрозы, указанные в статье 3 настоящего Соглашения;

18) выработка и реализация системы оценивания уязвимостей в области информационной безопасности и их устранения каждой из Сторон;

19) любые другие направления сотрудничества, которые могут быть дополнительно определены Сторонами.

Статья 3

Угрозы в области обеспечения международной информационной безопасности

Следующие способы использования информационных и коммуникационных технологий квалифицируются как угрозы в области обеспечения международной информационной безопасности, которым Стороны должны противодействовать в рамках данного Соглашения:

1) для осуществления действий, направленных на нарушение национального суверенитета, подрыв национальной безопасности, нарушение территориальной целостности Российской Федерации и Республики Индонезии и (или) представляющих угрозу миру, безопасности и стратегической безопасности;

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

3) для действий, направленных на вмешательство во внутренние дела, нарушающих общественный порядок, разжигающих вражду, основанную на этнических, расовых, политических и религиозных противоречиях, пропагандирующих расистские и ксенофобские идеи, порождающие ненависть, дискриминацию и насилие, нестабильность, а также для дестабилизации внутривнутриполитической 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 вредоносной информации, которая наносит ущерб общественно-политической и социально-экономической системе, духовной, нравственной и культурной среде.

Статья 4

Назначение координирующих органов

В целях эффективной реализации положений настоящего Соглашения и установления непосредственного взаимодействия Российской Федерации и Республики Индонезии в рамках настоящего

Соглашения Стороны назначают свои соответствующие координирующие органы, а именно:

от Российской Федерации - аппарат Совета Безопасности Российской Федерации;

от Республики Индонезии - Национальное агентство по кибербезопасности и криптографии Республики Индонезии.

В случае если Сторона меняет свой координирующий орган, она должна незамедлительно информировать другую Сторону о таких изменениях в письменной форме по дипломатическим каналам.

Статья 5

Формы и механизмы сотрудничества

1. В течение 60 дней с даты вступления настоящего Соглашения в силу Стороны обмениваются по дипломатическим каналам сведениями о компетентных органах Российской Федерации и Республики Индонезии, ответственных за реализацию настоящего Соглашения.

2. Стороны проводят регулярные консультации как на уровне уполномоченных лиц, так и на рабочем (экспертном) уровне с целью рассмотрения хода выполнения настоящего Соглашения, обмена данными и информацией, представляющими предмет общей заинтересованности, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы.

3. Такие консультации проводятся ежегодно как на уровне уполномоченных лиц, так и на рабочем (экспертном) уровне в Российской Федерации и Республике Индонезии на ротационной основе.

В случае необходимости каждая Сторона может предложить дополнительные консультации, дату, место их проведения и повестку дня.

4. Стороны могут договориться об особых механизмах выполнения настоящего Соглашения в целях дальнейшего содействия работе по конкретным направлениям сотрудничества, предусмотренным Соглашением, по линии компетентных органов Российской Федерации и Республики Индонезии. Стороны могут также договариваться о механизмах выполнения настоящего Соглашения между своими иными компетентными органами с целью содействия развитию конкретных направлений сотрудничества в рамках Соглашения.

Статья 6 Защита информации

1. 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 Российской Федерации и законодательством Республики Индонезии.

2. 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.

3. Настоящее Соглашение не налагает на Стороны обязательства по предоставлению информации и не предоставляет основу для передачи информации в рамках настоящего Соглашения, если раскрытие такой информации может нанести ущерб национальным интересам.

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, как это предусматривают законодательство Российской Федерации и законодательство Республики Индонезии.

Статья 8 Отношение к другим международным договорам

1. Стороны осуществляют сотрудничество с соблюдением законодательства Российской Федерации и законодательства Республики Индонезии, а также общепризнанных норм и принципов международного права.

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

Статья 9 Разрешение споров

Стороны решают любые спорные вопросы, которые могут возникнуть между ними 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 Поправки

Стороны в случае необходимости могут вносить поправки в настоящее Соглашение в любое время по обоюдному согласию посредством подписания дополнительных протоколов или обмена нотами. Такие поправки вступают в силу в день, который будет определен Сторонами, и становятся неотъемлемой частью настоящего Соглашения.

Статья 11 Вступление в силу, срок действия и прекращение действия Соглашения

1. Настоящее Соглашение 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. Настоящее Соглашение остается в силе в течение 5 лет и его действие автоматически продлевается на каждые последующие 5-летние периоды, пока одна из Сторон не решит расторгнуть настоящее Соглашение путем письменного уведомления другой Стороны по дипломатическим каналам за 90 дней до истечения соответствующего периода действия настоящего Соглашения.

3. 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, но не завершенных к моменту прекращения действия Соглашения.

В удостоверение чего нижеподписавшиеся, будучи надлежащим образом уполномоченными соответствующими правительствами, подписали настоящее Соглашение.

Совершено в г. " " 20 г., в двух экземплярах, на русском, индонезийском и английском языках, причем все тексты имеют одинаковую силу. В случае разногласий в толковании положений настоящего Соглашения используется текст на английском языке.

За Правительство
Российской Федерации

За Правительство
Республики Индонезии
