ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 18 ноября 2020 г. № 3023-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Никарагуа 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 и согласованный с другими заинтересованными федеральными органами исполнительной власти, аппаратом Совета Безопасности Российской Федерации и предварительно проработанный с Никарагуанской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Республики Никарагуа о сотрудничестве в области обеспечения международной информационной безопасности (прилагается).

Поручить МИДу России провести переговоры с Никарагуанской 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 М.Мишустин

4768088

Проект

СОГЛАШЕНИЕ

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

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

отмечая значительный прогресс 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 угрозами, связанными с возможностями использования таких технологий в целях, не совместимых 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 межконфессиональной вражды,

придавая важное значение международной информационной безопасности как одному из ключевых элементов 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 юрисдикцию государств над информационной инфраструктурой на их территориях, а также что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью "Интернет", включая обеспечение безопасности,

будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия Сторон 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,

стремясь предотвращать угрозы международной информационной безопасности, обеспечить интересы информационной безопасности государств Сторон в целях формирования международной информационной среды, для которой характерны мир, безопасность, открытость и сотрудничество,

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

согласились о нижеследующем:

Статья 1
Основные угрозы в области обеспечения международной информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основной угрозой в области обеспечения международной 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 оказания деструктивного воздействия на объекты информационной инфраструктуры;

3) в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности;

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

5) для вмешательства во внутренние дела 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 и социально-экономической обстановки, нарушения управления государством;

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

Статья 2
Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 1 настоящего Соглашения, Стороны, уполномоченные представители и компетентные органы государств Сторон, которые определяются в соответствии со статьей 4 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) определение, согласование и осуществление необходимого взаимодействия для обеспечения международной информационной безопасности;

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

3) противодействие угрозам в области обеспечения международной информационной безопасности, указанным в статье 1 настоящего Соглашения;

4) обмен информацией и взаимодействие в правоохранительной области в целях предупреждения, выявления и пресечения компьютерных инцидентов, а также расследования правонарушений и уголовных дел, связанных с использованием информационно-коммуникационных технологий в террористических и криминальных целях;

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

6) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения 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) содействие совершенствованию двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в обеспечении международной информационной безопасности;

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

10) углубление взаимодействия и координации деятельности государств Сторон по проблемам обеспечения международной информационной безопасности в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Международную организацию по стандартизации и другие);

11) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон в сфере международной информационной безопасности.

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

Статья 3
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 взаимного уважения суверенитета и территориальной целостности, мирного урегулирования споров и конфликтов, неприменения силы и угрозы силой, 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 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 4
Основные формы и механизмы сотрудничества

1. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии компетентных органов государств Сторон, ответственных за реализацию настоящего Соглашения. В течение 60 дней со дня вступления настоящего Соглашения в силу Стороны обменяются по дипломатическим каналам данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения.

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

3. С целью рассмотрения хода реализации настоящего Соглашения, 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 на регулярной основе консультации уполномоченных представителей и компетентных органов государств Сторон.

Указанные консультации проводятся по согласованию Сторон, как правило, два раза в год попеременно в Российской Федерации и Республике Никарагуа.

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

Статья 5
Защита информации

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

2. Стороны обязуются не раскрывать и не передавать без предварительного письменного согласия другой Стороны третьей стороне информацию о сотрудничестве, полученную или совместно созданную в рамках реализации настоящего Соглашения.

3. Необходимость сохранения в тайне отдельных аспектов сотрудничества между государствами Сторон или других сведений о сотрудничестве заблаговременно доводится одной Стороной до сведения другой Стороны.

4. Любая информация, передаваемая в рамках настоящего Соглашения, используется исключительно в его целях. Информация, полученная одной из Сторон в рамках сотрудничества, 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 Республики Никарагуа о взаимной защите секретной информации от 14 февраля 2010 г.

Статья 6
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 7
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 8
Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и 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. " " 20 г. в двух экземплярах на русском и испанском языках, причем оба текста имеют одинаковую силу.

За Правительство Российской Федерации	За Правительство Республики Никарагуа