ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 4 декабря 2023 г. № 3463-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Союз Мьянма 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 заинтересованными органами государственной власти и предварительно проработанный с Мьянманской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Республики Союз Мьянма о сотрудничестве в области обеспечения международной информационной безопасности (прилагается).

Поручить МИДу России провести переговоры с Мьянманской Стороной, разрешив вносить в прилагаемый проект изменения, не имеющие принципиального характера. По достижении договоренности уполномочить Секретаря Совета Безопасности Российской Федерации Патрушева Н.П. подписать от имени Правительства Российской Федерации указанное Соглашение.

Председатель Правительства
Российской Федерации

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
00A549C6D7F67C9AF7E29CB2C918EA03EF
Действителен с 07.03.2023 по 30.05.2024
Владелец: Правительство Российской Федерации

М.Мишустин

Проект

С О Г Л А Ш Е Н И Е

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

Правительство Российской Федерации и Правительство Республики Союз Мьянма, 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 информационно-коммуникационных 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 межконфессиональной вражды,

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

подтверждая то, 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 то, что государство имеет суверенное право определять и проводить государственную политику по вопросам, связанным с информационно-телекоммуникационной сетью "Интернет", включая обеспечение ее безопасного и стабильного функционирования,

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 национальные интересы в области 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

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

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

б) для осуществления компьютерных атак на объекты критической информационной инфраструктуры (определение дано в приложении к настоящему Соглашению, являющемся его неотъемлемой частью);

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

г) в иных преступных целях;

д) 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;

е) для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств, а также приводящей к возникновению угрозы жизни и безопасности граждан или к наступлению тяжких последствий;

ж) для выдвижения одними государствами против других государств необоснованных обвинений в организации и (или) совершении вредоносной деятельности в информационном пространстве.

2. Негативным фактором, оказывающим влияние на международную информационную безопасность, является отсутствие общепризнанного международного правового механизма деанонимизации информационного пространства.

3. Стороны могут по взаимной договоренности вносить изменения в перечень основных угроз в области обеспечения международной информационной безопасности, в частности, путем его дополнения и (или) актуализации в соответствии со статьей 9 настоящего Соглашения.

Статья 2
Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 1 настоящего Соглашения, Стороны и 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:

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

б) осуществление мониторинга возникающих угроз в сфере международной информационной безопасности и реагирование на них;

в) разработка и продвижение норм международного права и правил поведения государств в информационном пространстве в целях обеспечения национальной и международной информационной безопасности;

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

д) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения информационной безопасности в целях обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов (определение дано в приложении к настоящему Соглашению, являющемся его неотъемлемой частью);

е) взаимодействие в правоохранительной сфере по предупреждению, выявлению, пресечению и расследованию правонарушений и преступлений, связанных с использованием информационно-коммуникационных технологий в террористических, экстремистских и иных преступных целях;

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

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

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

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

л) 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, Международную организацию уголовной полиции - Интерпол и другие);

м) содействие научным исследованиям в области обеспечения международной информационной безопасности;

н) создание условий и содействие в подготовке специалистов, обмене студентами, аспирантами и преподавателями профильных высших учебных заведений государств Сторон в области обеспечения международной информационной безопасности;

о) проведение рабочих встреч, конференций, семинаров и других форумов 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 каждого из 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.

4. Стороны прилагают усилия к тому, чтобы информационная инфраструктура и ресурсы государств Сторон не использовались третьей стороной для нанесения ущерба государствам Сторон.

5. Стороны осуществляют взаимодействие в области противодействия преступности в сфере использования информационно-коммуникационных технологий без ущерба духу и положениям настоящего Соглашения.

6. Стороны не допускают трансграничный доступ к компьютерной информации, хранящейся в информационных системах одной из Сторон, без официального взаимодействия с правоохранительными органами соответствующей Стороны. Такое взаимодействие может осуществляться, в частности, в рамках двусторонних и многосторонних международных

договоров, в том числе о правовой помощи по уголовным делам, а также в рамках международного полицейского сотрудничества.

Статья 4
Координирующие органы

В целях содействия эффективной реализации положений настоящего Соглашения и установления непосредственного взаимодействия между Российской Федерацией и Республикой Союз Мьянма в рамках настоящего Соглашения координирующими органами определены:

от Российской Федерации - Министерство иностранных дел Российской Федерации;

от Республики Союз Мьянма - Министерство транспорта и коммуникаций Республики Союз Мьянма.

При необходимости Стороны могут заменить координирующий орган, незамедлительно оповестив в письменной форме о таких изменениях другую Сторону по дипломатическим каналам.

Статья 5
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 обмениваются по дипломатическим каналам данными о компетентных органах государств Сторон, ответственных за реализацию настоящего Соглашения. В случае изменения компетентных органов Стороны незамедлительно уведомляют друг друга об этом по дипломатическим каналам.

2. После обмена данными в соответствии с порядком, указанным в пункте 1 настоящей статьи, Стороны в течение 180 дней согласовывают план реализации основных направлений сотрудничества, указанных в статье 2 настоящего Соглашения. Уровень, сроки и место подписания данного плана, не являющегося международным договором, согласовываются по дипломатическим каналам.

3. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям компетентные органы

государств Сторон могут заключать соответствующие договоры межведомственного характера.

4. 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 компетентных органов государств Сторон.

5. Указанные консультации проводятся по согласованию Сторон, как правило, один раз в год, попеременно в Российской Федерации и Республике Союз Мьянма.

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

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. Стороны обязуются не раскрывать и не передавать без предварительного письменного согласия другой Стороны третьей стороне информацию, 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 Союза Мьянма о взаимной защите секретной информации от 3 апреля 2006 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

Любые спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, решаются путем консультаций и переговоров между Сторонами.

Статья 9
Изменения и дополнения

В настоящее Соглашение по взаимному письменному согласию Сторон могут вноситься изменения и дополнения, являющиеся его неотъемлемой частью и оформляемые отдельными протоколами.

Статья 10
Вступление в силу, срок действия и прекращение действия

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 вступления настоящего Соглашения в силу.

2. Настоящее Соглашение остается в силе в течение 5 лет. Его действие автоматически продлевается на каждые последующие 5-летние периоды, если ни одна из Сторон не уведомит другую Сторону по дипломатическим каналам в письменной форме о своем намерении прекратить действие настоящего Соглашения.

3. Действие настоящего Соглашения может быть прекращено одной из Сторон в любое время после передачи письменного уведомления по дипломатическим каналам не позднее чем за 90 дней до даты предполагаемого прекращения действия 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 подлинных экземплярах, каждый на русском, бирманском и английском языках, причем все тексты имеют одинаковую силу.

В случае разногласий в толковании положений настоящего Соглашения будет использоваться текст на английском языке.

За Правительство Российской Федерации	За Правительство Республики Союз Мьянма

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

П Е Р Е Ч Е Н Ь

основных понятий, используемых для целей взаимодействия сторон в ходе выполнения Соглашения между Правительством Российской Федерации и Правительством Республики Союз Мьянма о сотрудничестве в области обеспечения международной информационной безопасности

"Компьютерная атака" - целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической 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.

"Компьютерный инцидент" - факт нарушения и (или) прекращения функционирования объекта критической 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.

_____