ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 22 июля 2024 г. № 1953-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Лаосской Народно-Демократической Республики о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий

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 Лаосской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Лаосской Народно-Демократической Республики о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий (прилагается).

Поручить МИДу России провести переговоры с Лаосской 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

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
4E4B48AC2B4A4793191877D128ED7D62
Действителен с 03.05.2024 по 27.07.2025
Владелец: Правительство Российской Федерации

М.Мишустин

Проект

С О Г Л А Ш Е Н И Е

между Правительством Российской Федерации и Правительством Лаосской Народно-Демократической Республики о сотрудничестве в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий

Правительство Российской Федерации и Правительство Лаосской Народно-Демократической Республики, 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 безопасности в сфере использования информационно-коммуникационных технологий 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 в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий, обеспечить национальные интересы в области безопасности в сфере использования информационно-коммуникационных технологий 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 безопасности в сфере использования информационно-коммуникационных технологий,

согласились о нижеследующем:

Статья 1
Основные угрозы в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий

1. При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий являются:

1) использование информационно-коммуникационных технологий для осуществления актов, направленных на нарушение суверенитета, безопасности и территориальной целостности государств;

2) использование информационно-коммуникационных технологий для осуществления компьютерных атак на объекты критической информационной инфраструктуры;

3) использование информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности;

4) использование информационно-коммуникационных технологий в иных преступных целях;

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

7) использование информационно-коммуникационных технологий для распространения под видом достоверных сообщений заведомо ложной информации, приводящего к возникновению угрозы жизни и безопасности граждан или к наступлению тяжких последствий;

8) использование информационно-коммуникационных технологий для выдвижения одними государствами против других государств необоснованных обвинений в организации и (или) совершении преступлений, а также компьютерных атак.

2. Стороны могут по взаимной договоренности вносить изменения в перечень основных угроз в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий, в частности путем его дополнения и (или) актуализации в соответствии со статьей 8 настоящего Соглашения.

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 безопасности в сфере использования информационно-коммуникационных технологий по следующим основным направлениям:

1) определение, согласование и осуществление необходимого взаимодействия для обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

2) осуществление мониторинга возникающих угроз в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий и реагирование на них;

3) разработка и продвижение норм международного права, а также правил, норм и принципов ответственного поведения государств в информационно-коммуникационной среде в целях обеспечения национальной и международной безопасности в сфере использования информационно-коммуникационных технологий;

4) противодействие основным угрозам в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий, указанным в статье 1 настоящего Соглашения;

5) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения безопасности в сфере использования информационно-коммуникационных технологий в целях обнаружения, предупреждения и ликвидации последствий ИКТ-инцидентов. Для целей настоящего Соглашения под ИКТ-инцидентом Стороны понимают 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;

6) 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;

7) разработка и осуществление необходимых совместных мер доверия, способствующих обеспечению безопасности в сфере использования информационно-коммуникационных технологий;

8) обмен информацией о законодательстве каждого из государств Сторон по вопросам обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

9) содействие совершенствованию двусторонней нормативно-правовой базы и практических механизмов сотрудничества государств Сторон в обеспечении безопасности в сфере использования информационно-коммуникационных технологий;

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

11) углубление взаимодействия и координации деятельности государств Сторон по проблемам обеспечения безопасности в сфере использования информационно-коммуникационных технологий в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Международную организацию по стандартизации, Международную организацию уголовной полиции - Интерпол и др.);

12) содействие научным исследованиям в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

13) содействие в подготовке специалистов, обмене студентами, аспирантами и преподавателями профильных высших учебных заведений государств Сторон в области обеспечения безопасности в сфере использования информационно-коммуникационных технологий;

14) проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов государств Сторон по тематике безопасности в сфере использования информационно-коммуникационных технологий.

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 безопасности в сфере использования информационно-коммуникационных технологий 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
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. 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 этого 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 безопасности в сфере использования информационно-коммуникационных технологий, 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, один раз в год, попеременно в Российской Федерации и Лаосской Народно-Демократической Республике.

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 рамках настоящего Соглашения информации, доступ к которой ограничен в соответствии с законодательством каждого из 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 целях настоящего

Соглашения. 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 каждого из государств Сторон.

6. Порядок передачи и защиты секретной информации определяется Соглашением между Правительством Российской Федерации и Правительством Лаосской Народно-Демократической Республики о взаимной защите секретной информации от 17 декабря 2015 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 каждого из государств Сторон.

Статья 7
Разрешение споров

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

Статья 8
Изменения и дополнения

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

Статья 9
Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на тридцатый день со дня получения

по дипломатическим каналам последнего письменного уведомления о выполнении Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

2. 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.

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 и не завершенных к моменту прекращения действия настоящего Соглашения.

Совершено в г. " " 20 г. в двух подлинных экземплярах, каждый на русском, лаосском 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 Лаосской Народно-Демократической Республики