



ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 14 сентября 2021 г. № 2564-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Таджикистан 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 и аппаратом Совета Безопасности Российской Федерации и предварительно проработанный с Таджикистанской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Республики Таджикистан о сотрудничестве в области обеспечения международной информационной безопасности (прилагается).

Поручить МИДу России провести переговоры с Таджикистанской 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

СОГЛАШЕНИЕ

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

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

отмечая значительный прогресс в развитии и внедрении информационно-коммуникационных технологий, формирующих глобальное информационное пространство, оказывающих существенное влияние на обеспечение международной информационной безопасности,

отмечая большое значение информационно-коммуникационных технологий для социально-экономического развития на благо человечества, а также для поддержания международного мира, безопасности и стабильности,

выражая озабоченность угрозами, связанными с возможностями использования информационно-коммуникационных 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 внутривнутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды,

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

поддерживая разработку и принятие под эгидой Организации Объединенных Наций правил, норм и принципов ответственного поведения государств в информационном пространстве для содействия обеспечению равной безопасности для всех стран,

подтверждая, что государственный суверенитет и международные нормы и принципы распространяются на деятельность государств, связанную с использованием информационно-коммуникационных технологий, и юрисдикцию государств над информационной инфраструктурой на их территории, а также суверенное право государств

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 настоящей необходимостью и отвечают их интересам,

основываясь на резолюции Генеральной Ассамблеи Организации Объединенных Наций 73/27 "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности" от 5 декабря 2018 г.,

придавая важное значение балансу между обеспечением безопасности и соблюдением прав и свобод человека и гражданина в области использования информационно-коммуникационных технологий,

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

желая создать, исходя из взаимного уважения независимости, суверенитета, интересов и территориальной целостности, правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности, которое не направлено на причинение вреда интересам третьей стороны,

согласились о нижеследующем:

Статья 1 Основные понятия

Для целей взаимодействия Сторон в ходе выполнения настоящего Соглашения используются основные понятия, предусмотренные Соглашением между правительствами государств - членом Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности от 16 июня 2009 г. и Шанхайской конвенцией о борьбе с терроризмом, сепаратизмом и экстремизмом от 15 июня 2001 г.

Статья 2

Основные угрозы в области обеспечения международной информационной безопасности

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:

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

2) для оказания деструктивного воздействия на объекты критической информационной инфраструктуры;

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

4) в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

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 внутрисполитической и социально-экономической обстановки, нарушения управления государством;

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

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 государств Сторон, было совместимо с задачами поддержания международной безопасности и стабильности и соответствовало общепризнанным принципам и нормам международного права, включая принципы взаимного уважения

государственного 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 законодательством государств Сторон.

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 для нанесения ущерба интересам государств Сторон.

Статья 4

Основные направления сотрудничества

1. С учетом основных угроз Стороны, компетентные органы государств Сторон, которые определяются в соответствии со статьей 6 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1) координация противодействия угрозам в области обеспечения международной информационной безопасности, указанным в статье 2 настоящего Соглашения;

2) взаимодействие в правоохранительной области в целях выявления, предупреждения, пресечения и расследования правонарушений и преступлений, связанных с использованием информационно-коммуникационных технологий в террористических, экстремистских и иных криминальных целях;

3) согласование и осуществление необходимых мер доверия, способствующих обеспечению международной информационной безопасности;

4) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения информационной безопасности;

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

6) совершенствование двусторонней нормативной правовой базы и практических механизмов сотрудничества государств Сторон в области обеспечения международной информационной безопасности;

7) участие в разработке и продвижении норм международного права в целях обеспечения национальной и международной информационной безопасности;

8) взаимодействие и координация деятельности государств Сторон при решении проблем обеспечения международной информационной безопасности в рамках международных организаций и форумов (включая Организацию Объединенных Наций, Международный союз электросвязи, Организацию по безопасности и сотрудничеству в Европе, Шанхайскую организацию сотрудничества, Организацию Договора о коллективной безопасности, Содружество Независимых Государств и др.);

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

10) взаимодействие в области подготовки кадров, стажировок, обмена специалистами.

2. Стороны или компетентные органы государств Сторон могут определять другие направления сотрудничества путем письменной договоренности.

Статья 5

Координирующие органы

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

от Российской Федерации - аппарат Совета Безопасности Российской Федерации;

от Республики Таджикистан - аппарат Совета Безопасности Республики Таджикистан.

Статья 6

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.

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

3. В целях рассмотрения хода реализации настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз международной информационной безопасности, определения, согласования и координации совместных мер реагирования на такие угрозы координирующие органы проводят на регулярной основе межведомственные консультации с участием представителей компетентных органов государств Сторон, а также консультации компетентных органов государств Сторон.

Межведомственные консультации проводятся по согласованию координирующих органов Сторон не реже одного раза в год попеременно в Российской Федерации и Республике Таджикистан, консультации компетентных органов - по их согласованию.

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

Статья 7

Защита информации

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.

Защита такой информации осуществляется в соответствии с законодательством и (или) соответствующими нормативными правовыми актами государства получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия и соблюдения условий предоставившей Стороны.

Такая информация обозначается в соответствии с законодательством и международными договорами государств Сторон, а факты ее передачи между Сторонами фиксируются документально.

Стороны не допускают трансграничный доступ к компьютерной информации, хранящейся в информационных системах одной из Сторон, без официального взаимодействия с правоохранительными органами соответствующей Стороны.

Порядок обмена, условия и меры по защите информации, содержащей сведения, составляющие государственную тайну Российской Федерации и (или) государственные секреты Республики Таджикистан, в ходе реализации и по окончании действия настоящего Соглашения определяются Соглашением между Правительством Российской Федерации и Правительством Республики Таджикистан о взаимной защите секретной информации от 22 января 2003 г.

Статья 8 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 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 государств Сторон и в случае необходимости по дипломатическим каналам.

