ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

РАСПОРЯЖЕНИЕ

от 26 февраля 2022 г. № 332-р

МОСКВА

О подписании Соглашения между Правительством Российской Федерации и Правительством Республики Сербии о сотрудничестве в области обеспечения 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 Генеральной прокуратурой Российской Федерации и предварительно проработанный с Сербской Стороной проект Соглашения между Правительством Российской Федерации и Правительством Республики Сербии о сотрудничестве в области обеспечения информационной безопасности (прилагается).

Поручить Секретарю Совета Безопасности Российской Федерации Патрушеву Н.П. провести переговоры с Сербской 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

5502483

Проект

СОГЛАШЕНИЕ

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

Правительство Российской Федерации и Правительство Республики Сербии, 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 внутриполитической и социально-экономической обстановки, разжигания межнациональной и межконфессиональной вражды,

придавая важное значение 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, 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 настоятельной 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 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 информационной безопасности, которое не направлено на причинение вреда интересам третьей стороны,

согласились о нижеследующем:

Статья 1
Основные угрозы в области обеспечения информационной безопасности

При осуществлении сотрудничества в соответствии с настоящим Соглашением Стороны исходят из того, что основными угрозами в области обеспечения информационной безопасности являются:

1) использование информационно-коммуникационных технологий в военно-политической и иных сферах в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

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

3) использование информационно-коммуникационных технологий в экстремистских целях, а также для вмешательства во внутренние дела суверенных государств;

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

5) использование информационно-коммуникационных технологий в преступных целях, в том числе для совершения преступлений в сфере компьютерной информации, а также для совершения различных видов мошенничества;

6) использование информационно-коммуникационных технологий для проведения компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру;

7) использование отдельными государствами технологического доминирования в глобальном информационном пространстве для монополизации рынка информационно-коммуникационных технологий, ограничения доступа других государств к передовым информационно-коммуникационным технологиям, а также для усиления их технологической зависимости от доминирующих в сфере информатизации государств и информационного неравенства.

Статья 2
Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения 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 3
Основные направления сотрудничества

1. С учетом основных угроз, указанных в статье 1 настоящего Соглашения, Стороны, компетентные органы государств Сторон, которые определяются в соответствии со статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения информационной безопасности по следующим основным направлениям:

1) противодействие угрозе использования информационно-коммуникационных технологий в целях подрыва (ущемления) суверенитета, нарушения территориальной целостности государств, осуществления в глобальном информационном пространстве иных действий, препятствующих поддержанию международного мира, безопасности и стабильности;

2) противодействие угрозе использования информационно-коммуникационных технологий в террористических целях, в том числе для пропаганды терроризма и привлечения к террористической деятельности новых сторонников;

3) противодействие угрозе использования информационно-коммуникационных технологий в экстремистских целях, а также в целях вмешательства во внутренние дела государств Сторон;

4) противодействие угрозе использования информационно-коммуникационных технологий в преступных целях;

5) противодействие угрозе использования информационно-коммуникационных технологий для проведения компьютерных атак на

информационные ресурсы государств Сторон, в том числе на критическую информационную инфраструктуру;

6) взаимодействие органов государств Сторон, уполномоченных в области реагирования на компьютерные инциденты, включая обмен информацией о передовых практиках обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы государств, в том числе на критическую информационную инфраструктуру, а также реагирования на компьютерные инциденты;

7) содействие обеспечению технологического суверенитета государств Сторон в области информационно-коммуникационных технологий;

8) согласование и осуществление необходимых мер укрепления доверия, способствующих обеспечению информационной безопасности;

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

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

11) согласование позиций и координация действий государств Сторон на профильных площадках международных организаций и форумов, направленных на содействие:

а) формированию системы обеспечения международной информационной безопасности;

б) организации под эгидой Организации Объединенных Наций регулярного институционального диалога с участием всех государств - членов Организации Объединенных Наций для обеспечения демократического, инклюзивного и транспарентного переговорного процесса по вопросам безопасности в сфере использования информационно-коммуникационных технологий;

в) выработке с учетом специфики информационно-коммуникационных технологий новых принципов и норм международного права, регулирующих деятельность государств в глобальном информационном пространстве;

г) обеспечению безопасного и стабильного функционирования и развития информационно-телекоммуникационной сети "Интернет" на основе равноправного участия государств - членов мирового сообщества в управлении этой сетью и повышению роли Международного союза электросвязи в таком управлении;

12) проведение рабочих встреч, конференций, семинаров и других форумов с участием экспертов компетентных органов государств Сторон в области обеспечения информационной безопасности;

13) взаимодействие в области подготовки кадров, стажировок, обмена специалистами в области обеспечения информационной безопасности.

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

Статья 4
Координирующие органы

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

от Российской Федерации - аппарат Совета Безопасности Российской Федерации;

от Республики Сербии - Министерство внутренних дел Республики Сербии.

Статья 5
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 международные договоры.

3. В целях рассмотрения хода реализации настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз 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 Сербии, 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 6
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 секретной информации в ходе реализации и по окончании действия настоящего Соглашения определяются Соглашением между Правительством Российской Федерации и Правительством Республики Сербии о взаимной защите секретной информации от 16 октября 2014 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

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 9
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. По согласию Сторон в настоящее Соглашение могут вноситься изменения, являющиеся неотъемлемой частью настоящего Соглашения и оформляемые отдельными протоколами.

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. " " 202 г. в двух экземплярах, каждый на русском и сербском языках, причем оба текста имеют одинаковую силу.

За Правительство Российской Федерации	За Правительство Республики Сербии