

**СОГЛАШЕНИЕ**  
**между Правительством Российской Федерации**  
**и Правительством Республики Зимбабве**  
**о сотрудничестве в области обеспечения**  
**международной информационной безопасности**

Правительство Российской Федерации и Правительство Республики Зимбабве (далее совместно именуемые «Стороны» и индивидуально «Сторона»),

подтверждая с учетом итогов первого саммита Россия-Африка (Сочи, 24 октября 2019 г.) твердый настрой на поступательное развитие всестороннего взаимодействия между Российской Федерацией и африканскими государствами,

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, 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,

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 территории, а также то, что государство имеет суверенное право определять и проводить 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 интересам государств Сторон,

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:

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

2) для осуществления компьютерных атак на объекты критической информационной инфраструктуры;

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

4) в иных преступных целях;

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 внутривнутриполитической 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;

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

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

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 8 настоящего Соглашения.

## Статья 2

### Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество в области обеспечения международной информационной безопасности в рамках настоящего Соглашения. Такое сотрудничество будет способствовать социально-экономическому развитию и будет совместимо с задачами поддержания международного мира, безопасности и стабильности, будет соответствовать 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 Сторон 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. Стороны имеют 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 3

#### Основные направления сотрудничества

1. С учетом основных угроз в области обеспечения международной информационной безопасности, 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) осуществление мониторинга возникающих угроз в сфере международной информационной безопасности и реагирование на них;

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

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

5) обмен информацией между компетентными органами государств Сторон по вопросам обеспечения информационной безопасности в целях обнаружения, предупреждения и ликвидации последствий компьютерных инцидентов;

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 международной информационной безопасности;

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

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

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 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);

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

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

14) 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 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 шестидесяти (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 ста восьмидесяти (180) дней согласовывают план реализации основных направлений сотрудничества, указанных в статье 3 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. В целях 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.

5. Консультации, указанные в пункте 4 настоящей статьи, проводятся по согласованию Сторон, как правило, один раз в год, попеременно на территории государств Сторон.



6. 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 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 взаимной передачи и защиты сведений, составляющих государственную тайну государств Сторон, определяется отдельным международным договором.

## 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

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 (30-й) 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 девяноста (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.

В удостоверение чего нижеподписавшиеся, должным образом уполномоченные представители Сторон, подписали настоящее Соглашение.

Совершено в г. Санкт-Петербурге " 27 " июля 2023 г.  
в двух (2) подлинных экземплярах, каждый на русском и английском языках, причем оба текста имеют одинаковую силу.

**За Правительство  
Российской Федерации**



**За Правительство  
Республики Зимбабве**

