

# Конвенция об обеспечении международной информационной безопасности (концепция)

## ПРЕАМБУЛА

Государства-участники настоящей Конвенции, отмечая значительный прогресс в развитии информационно-коммуникационных технологий и средств, формирующих информационное пространство,

*выражая* озабоченность угрозами, связанными с возможностями использования таких технологий и средств в целях, не совместимых с задачами обеспечения международной безопасности и стабильности, как в гражданской, так и в военной сферах,

*придавая* важное значение международной информационной безопасности как одному из ключевых элементов системы международной безопасности, будучи убежденными в том, что дальнейшее углубление доверия и развитие взаимодействия государств-участников в вопросах обеспечения международной информационной безопасности являются настоятельной необходимостью и отвечают их интересам,

*принимая* во внимание важное значение информационной безопасности для реализации основных прав и свобод человека и гражданина,

*учитывая* резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/65/41 от 8 декабря 2010 г. «Достижения в сфере информатизации и коммуникаций в контексте международной безопасности»,

*стремясь* ограничить угрозы международной информационной безопасности, обеспечить информационную безопасность государств-участников и создать информационное пространство, для которого характерны мир, сотрудничество и гармония,

*желая* создать правовые и организационные основы сотрудничества государств-участников в области обеспечения международной информационной безопасности,

*ссылаясь* на резолюцию Генеральной Ассамблеи Организации Объединенных Наций A/RES/55/29 от 20 ноября 2000 г. «Роль науки и техники в контексте международной безопасности и разоружения», в которой, в частности,

признается, что достижения науки и техники могут иметь как гражданское, так и военное применение, и что необходимо поддерживать и поощрять развитие науки и техники для использования в гражданских целях,

*признавая* необходимость предотвращения возможности использования информационно-коммуникационных технологий в целях, которые не совместимы с задачами обеспечения международной стабильности и

безопасности и способны оказать отрицательное воздействие на целостность государственных инфраструктур, нанося ущерб их безопасности,

*подчеркивая* необходимость усиления координации и укрепления сотрудничества между государствами в борьбе с преступным использованием информационных технологий и в этом контексте отмечая ту роль, которую могут сыграть Организация Объединенных Наций и другие международные и региональные организации,

*подчеркивая* важность безопасного, непрерывного и стабильного функционирования Интернета и необходимость защиты Интернета и других информационно-коммуникационных сетей от возможного неблагоприятного воздействия и подверженности угрозам,

*подтверждая* необходимость общего понимания вопросов безопасности Интернета и дальнейшего сотрудничества на национальном и международном уровнях,

*вновь подтверждая*, что политические полномочия по связанным с Интернетом вопросам государственной политики являются суверенным правом государств, и что государства имеют права и обязанности в отношении связанных с Интернетом вопросов государственной политики международного уровня,

*признавая*, что доверие и безопасность в использовании информационно-коммуникационных технологий относятся к фундаментальным основам информационного общества и что необходимо поощрять, формировать, развивать и активно внедрять устойчивую глобальную культуру кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи Организация Объединенных Наций A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»,

*отмечая* необходимость активизации усилий по преодолению «цифрового разрыва» путем облегчения передачи информационно-коммуникационных технологий развивающимся странам и наращивая их потенциал в вопросах передовой практики и профессиональной подготовки в области кибербезопасности, как отмечается в резолюции Генеральной Ассамблеи Организация Объединенных Наций A/RES/64/211 от 21 декабря 2009 г. «Создание глобальной культуры кибербезопасности и оценка национальных усилий по защите важнейших информационных инфраструктур»,

*будучи убеждены* в необходимости проведения в приоритетном порядке общей политики, нацеленной на защиту общества от правонарушений в информационном пространстве, в том числе путем принятия соответствующих законодательных актов и укрепления международного сотрудничества, *сознавая* глубокие перемены, вызванные внедрением цифровых технологий, объединением и продолжающейся глобализацией компьютерных сетей,

*будучи озабоченными* угрозой того, что компьютерные сети могут также использоваться для совершения уголовных преступлений, и что доказательства

совершения таких правонарушений могут храниться в этих сетях и передаваться по ним,

*признавая* необходимость сотрудничества между государствами и частным бизнесом в борьбе против правонарушений в информационном пространстве и необходимость защиты законных интересов в сфере использования и развития информационно-коммуникационных технологий,

*полагая*, что для эффективной борьбы против правонарушений в информационном пространстве требуется более широкое, оперативное и хорошо отлаженное международное сотрудничество в области противодействия правонарушениям,

*будучи убежденными* в том, что настоящая Конвенция необходима для противодействия нарушениям конфиденциальности, целостности и доступности компьютерных систем и сетей и компьютерной информации, а также злоупотреблениям такими системами, сетями и информацией путем обеспечения наказуемости таких деяний, описываемых в настоящей Конвенции, и предоставления полномочий, достаточных для эффективной борьбы с такими правонарушениями, путем содействия выявлению и расследованию таких правонарушений и преследованию за их совершение как на внутригосударственном, так и на международном уровнях и путем разработки договоренностей относительно оперативного и надежного международного сотрудничества,

*памятуя* о необходимости обеспечения должного баланса между интересами поддержания правопорядка и уважением основополагающих прав человека, как это предусмотрено Международным пактом о гражданских и политических правах 1966 года, а также другими международными договорами о правах человека, в которых подтверждается право каждого беспрепятственно придерживаться своих мнений и право на свободное выражение своего мнения, включая свободу искать, получать и распространять всякого рода информацию и идеи, независимо от государственных границ,

*памятуя* также о праве на уважение частной жизни и защиту персональных данных,

*учитывая* положения Конвенции о правах ребенка 1989 года и Конвенции о запрещении и немедленных мерах по искоренению наихудших форм детского труда, принятой Генеральной конференцией Международной организации труда в 1999 году,

*приветствуя* события последнего времени, способствующие дальнейшему росту международного взаимопонимания и сотрудничества в борьбе с правонарушениями в информационном пространстве, включая меры, принятые Организацией Объединенных Наций, Шанхайской организацией сотрудничества, Европейским Союзом, Организацией Азиатско-Тихоокеанского сотрудничества, Организацией американских государств, Ассоциацией стран Юго-Восточной Азии, Организацией экономического сотрудничества и развития, «Группой восьми» и другими международными организациями и форумами,

согласились о нижеследующем:

## **Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ**

### **Статья 1. Предмет и цель Конвенции**

*Предметом* регулирования настоящей Конвенции является деятельность государств по обеспечению международной информационной безопасности. *Целью* настоящей Конвенции является противодействие использованию информационно-коммуникационных технологий для нарушения международного мира и безопасности, а также установление мер, способствующих тому, чтобы деятельность государств в информационном пространстве:

- 1) способствовала общему социальному и экономическому развитию;
- 2) осуществлялась таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности;
- 3) соответствовала общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы, невмешательства во внутренние дела, уважения прав и основных свобод человека;
- 4) была совместимой с правом каждого искать, получать и распространять информацию и идеи, как это зафиксировано в документах ООН, с учетом того, что такое право может быть ограничено законодательством для защиты интересов национальной и общественной безопасности каждого государства, а также для предотвращения неправомерного использования и несанкционированного вмешательства в информационные ресурсы;
- 5) гарантировала свободу технологического обмена и свободу обмена информацией с учетом уважения суверенитета государств и их существующих политических, исторических и культурных особенностей.

### **Статья 2. Термины и определения**

Для целей настоящей Конвенции используются следующие термины и определения:

**«доступ к информации»** - возможность получения информации и ее использования;

**«информационная безопасность»** - состояние защищенности интересов личности, общества и государства от угроз деструктивных и иных негативных воздействий в информационном пространстве;

**«информационная война»** - противоборство между двумя или более государствами в информационном пространстве с целью нанесения ущерба

информационным системам, процессам и ресурсам, критически важным и другим структурам, подрыва политической, экономической и социальной систем, массовой психологической обработки населения для дестабилизации общества и государства, а также принуждения государства к принятию решений в интересах противоборствующей стороны;

**«информационная инфраструктура»** - совокупность технических средств и систем формирования, преобразования, передачи, использования и хранения информации;

**«информационная система»** - совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

**«информационное оружие»** - информационные технологии, средства и методы, предназначенные для ведения информационной войны;

**«информационное пространство»** - сфера деятельности, связанная с формированием, созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие, в том числе на индивидуальное и общественное сознание, информационную инфраструктуру и собственно информацию;

**«информационно-коммуникационные технологии»** - совокупность методов, производственных процессов и программно-технических средств, интегрированных с целью формирования, преобразования, передачи, использования и хранения информации;

**«информационные ресурсы»** - информационная инфраструктура, а также собственно информация и ее потоки;

**«конфиденциальность информации»** - обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя;

**«критически важный объект информационной инфраструктуры»** - часть (элемент) информационной инфраструктуры, воздействие на которую может иметь последствия, непосредственно затрагивающие национальную безопасность, включая безопасность личности, общества и государства;

**«международная информационная безопасность»** - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве;

**«неправомерное использование информационных ресурсов»** - использование информационных ресурсов без соответствующих прав или с нарушением установленных правил, законодательства государств либо норм международного права;

**«несанкционированное вмешательство в информационные ресурсы»** - неправомерное воздействие на процессы формирования, обработки, преобразования, передачи, использования и хранения информации;

**«оператор информационной системы»** - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

**«правонарушение в информационном пространстве»** - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в противоправных целях;

**«предоставление информации»** - действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

**«распространение информации»** - действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

**«терроризм в информационном пространстве»** - использование информационных ресурсов и (или) воздействие на них в информационном пространстве в террористических целях;

**«угроза в информационном пространстве (угроза информационной безопасности)»** - факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.

### **Статья 3. Исключения в применении Конвенции**

Настоящая Конвенция не применяется в случаях, когда действия осуществлены в рамках информационной инфраструктуры одного государства, гражданином или юридическим лицом, находящимся под юрисдикцией этого государства, и последствия этих действий имели место только в отношении граждан и юридических лиц, находящихся под юрисдикцией этого же государства, и никакое другое государство не имеет оснований для осуществления своей юрисдикции.

### **Статья 4. Основные угрозы международному миру и безопасности в информационном пространстве**

В качестве основных угроз в информационном пространстве, приводящих к нарушению международного мира и безопасности, рассматриваются следующие:

1) использование информационных технологий и средств для осуществления враждебных действий и актов агрессии;

- 2) целенаправленное деструктивное воздействие в информационном пространстве на критически важные структуры другого государства;
- 3) неправомерное использование информационных ресурсов другого государства без согласования с государством, в информационном пространстве которого располагаются эти ресурсы;
- 4) действия в информационном пространстве с целью подрыва политической, экономической и социальной систем другого государства, психологическая обработка населения, дестабилизирующая общество;
- 5) использование международного информационного пространства государственными и негосударственными структурами, организациями, группами и отдельными лицами в террористических, экстремистских и иных преступных целях;
- 6) трансграничное распространение информации, противоречащей принципам и нормам международного права, а также национальным законодательствам государств;
- 7) использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду, расистских и ксенофобских письменных материалов, изображений или любого другого представления идей или теорий, которые пропагандируют, способствуют или подстрекают к ненависти, дискриминации или насилию против любой личности или группы лиц, если в качестве предлога к этому используются факторы, основанные на расе, цвете кожи, национальном или этническом происхождении, а также религии;
- 8) манипулирование информационными потоками в информационном пространстве других государств, дезинформация и сокрытие информации с целью искажения психологической и духовной среды общества, эрозия традиционных культурных, нравственных, этических и эстетических ценностей;
- 9) использование информационно-коммуникационных технологий и средств в ущерб основным правам и свободам человека, реализуемым в информационном пространстве;
- 10) противодействие доступу к новейшим информационно-коммуникационным технологиям, создание условий технологической зависимости в сфере информатизации в ущерб другим государствам;
- 11) информационная экспансия, приобретения контроля над национальными информационными ресурсами другого государства.

Дополнительными факторами, усиливающими опасность перечисленных угроз, являются:

- 1) неопределенность в идентификации источника враждебных действий, особенно с учетом возрастающей активности отдельных лиц, групп и

организаций, включая преступные организации, которые выполняют посреднические функции в осуществлении деятельности от имени других;

2) потенциальная опасность включения в информационно-коммуникационные технологии недекларируемых деструктивных возможностей;

3) различия в степени оснащенности информационно-коммуникационными технологиями и их безопасности в разных государствах («цифровое неравенство»);

4) различия в национальных законодательствах и практике формирования безопасной и быстро восстанавливающейся информационной инфраструктуры.

### **Статья 5. Основные принципы обеспечения международной информационной безопасности**

Информационное пространство является общечеловеческим достоянием. Его безопасность является основой обеспечения устойчивого развития мировой цивилизации.

В целях создания и поддержания атмосферы доверия в информационном пространстве необходимо соблюдение государствами-участниками следующих принципов:

1) деятельность каждого государства-участника в информационном пространстве должна способствовать социальному и экономическому развитию и осуществляться таким образом, чтобы быть совместимой с задачами поддержания международного мира и безопасности, соответствовать общепризнанным принципам и нормам международного права, включая принципы мирного урегулирования споров и конфликтов, неприменения силы в международных отношениях, невмешательства во внутренние дела других государств, уважения суверенитета государств, основных прав и свобод человека;

2) государства-участники в ходе формирования системы международной информационной безопасности будут руководствоваться принципом неделимости безопасности, означающим, что безопасность каждого из них неразрывно связана с безопасностью всех других государств и мирового сообщества в целом, а также не будут укреплять свою безопасность в ущерб безопасности других государств;

3) каждое государство-участник должно стремиться к преодолению различий в степени оснащенности национальных информационных систем современными информационно-коммуникационными технологиями, сокращению «цифрового разрыва» в целях снижения общего уровня угроз в информационном пространстве;

4) все государства-участники в информационном пространстве пользуются суверенным равенством, имеют одинаковые права и обязанности и являются



равноправными субъектами информационного пространства независимо от различий экономического, социального, политического или иного характера;

5) каждое государство-участник вправе устанавливать суверенные нормы и управлять в соответствии с национальными законами своим информационным пространством. Суверенитет и законы распространяются на информационную инфраструктуру, расположенную на территории государства-участника или иным образом находящуюся под его юрисдикцией. Государства-участники должны стремиться к гармонизации национальных законодательств, различия в них не должны создавать барьеры на пути формирования надежной и безопасной информационной среды;

6) каждое государство-участник должно придерживаться принципа ответственности за собственное информационное пространство, в том числе за его безопасность и за содержание размещаемой в нем информации;

7) каждое государство-участник имеет право свободно осуществлять без вмешательства извне развитие своего информационного пространства, и каждое другое государство обязано уважать это право в соответствии с принципом равноправия и самоопределения народов, закрепленного в Уставе Организации Объединенных Наций;

8) каждое государство-участник, учитывая законные интересы безопасности других государств, может свободно и самостоятельно определять свои интересы обеспечения информационной безопасности на основе суверенного равенства, а также свободно выбирать способы обеспечения собственной информационной безопасности в соответствии с международным правом;

9) государства-участники признают, что агрессивная «информационная война» составляет преступление против международного мира и безопасности;

10) информационное пространство государства-участника не должно быть объектом приобретения другим государством в результате угрозы силой или ее применения;

11) каждое государство-участник имеет неотъемлемое право на самооборону перед лицом агрессивных действий в информационном пространстве в отношении его при условии достоверного установления источника агрессии и адекватности ответных мер;

12) каждое государство-участник будет определять свой военный потенциал в информационном пространстве на основе национальных процедур с учетом законных интересов безопасности других государств, а также необходимости содействовать укреплению международного мира и безопасности. Ни одно из государств-участников не будет предпринимать попыток добиться господства в информационном пространстве над другими государствами;

13) государство-участник может размещать свои силы и средства обеспечения информационной безопасности на территории другого государства в

соответствии с соглашением, выработанным ими на добровольной основе в ходе переговоров, а также в соответствии с международным правом;

14) каждое государство-участник принимает необходимые меры для обеспечения невмешательства в деятельность международных информационных систем управления транспортными, финансовыми потоками, средствами связи, средствами международного информационного, в том числе научного и образовательного обмена, исходя из понимания того, что подобное вмешательство может негативно повлиять на информационное пространство в целом;

15) государства-участники должны поддерживать и стимулировать научно-технические разработки в области освоения информационного пространства, а также образовательно-просветительскую деятельность, направленную на формирование глобальной культуры кибербезопасности;

16) каждое государство-участник в рамках имеющихся средств обеспечивает в своем информационном пространстве соблюдение основных прав и свобод человека и гражданина, соблюдение прав на интеллектуальную собственность, включая патенты, технологии, коммерческую тайну, торговые марки и авторские права;

17) каждое государство-участник гарантирует свободу слова, выражение мнений в информационном пространстве, защиту от незаконного вмешательства в частную жизнь граждан;

18) каждое государство-участник стремится к соблюдению баланса между основными свободами и эффективным противодействием террористическому использованию информационного пространства;

19) государства-участники не вправе ограничивать или нарушать доступ граждан к информационному пространству, кроме как в целях защиты национальной и общественной безопасности, а также предотвращения неправомерного использования и несанкционированного вмешательства в национальную информационную инфраструктуру;

20) государства-участники стимулируют партнерство бизнеса и гражданского общества в информационном пространстве;

21) государства-участники признают свои обязанности по обеспечению осведомленности своих граждан, общественных и государственных органов, других государств и мирового сообщества о новых угрозах в информационном пространстве и об известных путях повышения уровня их безопасности.

## **Глава 2. ОСНОВНЫЕ МЕРЫ ПРЕДОТВРАЩЕНИЯ И РАЗРЕШЕНИЯ ВОЕННЫХ КОНФЛИКТОВ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ**

### **Статья 6. Основные меры предотвращения военных конфликтов в информационном пространстве**

Руководствуясь изложенными в Статье 5 принципами, государства-участники обязуются принимать меры к упреждающему выявлению потенциальных конфликтов в информационном пространстве, а также прилагать совместные усилия для их предотвращения, мирного урегулирования кризисов и споров. С этой целью государства-участники:

- 1) обязуются сотрудничать друг с другом в сфере обеспечения международной информационной безопасности для поддержания международного мира и безопасности и содействия международной экономической стабильности и прогрессу, общему благосостоянию народов и международному сотрудничеству, свободному от дискриминации;
- 2) будут предпринимать все необходимые меры для предотвращения деструктивного информационного воздействия со своей территории или с использованием информационной инфраструктуры, находящейся под его юрисдикцией, а также обязуются взаимодействовать для определения источника компьютерных атак, проведенных с использованием их территории, противодействия этим атакам и ликвидации последствий;
- 3) будут воздерживаться от разработки и принятия планов, доктрин, способных спровоцировать возрастание угроз в информационном пространстве, а также вызвать напряженность в отношениях между государствами и возникновение «информационных войн»;
- 4) будут воздерживаться от любых действий, направленных на полное или частичное нарушение целостности информационного пространства другого государства;
- 5) обязуются не использовать информационно-коммуникационные технологии для вмешательства в дела, относящиеся ко внутренней компетенции другого государства;
- 6) будут воздерживаться в международных отношениях от угрозы силой или ее применения против информационного пространства любого другого государства для его нарушения или в качестве средства разрешения конфликтов;
- 7) обязуются воздерживаться от организации или поощрения организации каких-либо иррегулярных сил для осуществления неправомерных действий в информационном пространстве другого государства;
- 8) обязуются воздерживаться от клеветнических утверждений, а также от оскорбительной или враждебной пропаганды для осуществления интервенции или вмешательства во внутренние дела других государств;
- 9) имеют право и обязуются бороться против распространения недостоверных или искаженных сообщений, которые могут рассматриваться как вмешательство во внутренние дела других государств или как наносящие ущерб международному миру и безопасности;

10) будут принимать меры по ограничению распространения «информационного оружия» и технологий его создания.

### **Статья 7. Меры, направленные на разрешение военных конфликтов в информационном пространстве**

1) Государства-участники разрешают конфликты в информационном пространстве, в первую очередь путем переговоров, обследования, посредничества, примирения, арбитража, судебного разбирательства, обращения к региональным органам или соглашениям или иными мирными средствами по своему выбору таким образом, чтобы не подвергать угрозе международный мир и безопасность.

2) В случае любого международного конфликта право государств-участников, находящихся в конфликте, выбирать методы или средства ведения «информационной войны» ограничено применимыми нормами международного гуманитарного права.

### **Глава 3. ОСНОВНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ИСПОЛЬЗОВАНИЮ ИНФОРМАЦИОННОГО ПРОСТРАНСТВА В ТЕРРОРИСТИЧЕСКИХ ЦЕЛЯХ**

#### **Статья 8. Использование информационного пространства в террористических целях**

Государства-участники осознают возможность использования информационного пространства для осуществления террористической деятельности.

#### **Статья 9. Основные меры противодействия использованию информационного пространства в террористических целях**

В целях противодействия использованию информационного пространства в террористических целях государства-участники:

1) принимают меры по противодействию использованию информационного пространства в террористических целях и признают для этого необходимость совместных решительных действий;

2) будут стремиться к выработке единых подходов к прекращению функционирования Интернет-ресурсов террористического характера;

3) осознают необходимость установления и расширения обмена информацией об угрозах совершения компьютерных атак, о признаках, фактах, методах и средствах использования сети Интернет в террористических целях, об устремлениях и деятельности террористических организаций в информационном пространстве, а также обмена опытом и лучшими практиками мониторинга информационных ресурсов сети Интернет, поиска и отслеживания содержимого сайтов террористической направленности, проведения

криминалистических компьютерных экспертиз в этой сфере, правового регулирования и организации деятельности по противодействию использованию информационного пространства в террористических целях;

4) принимают такие меры законодательного и иного характера, которые могут понадобиться для того, чтобы позволить компетентным органам проводить следственные, розыскные и иные процессуальные мероприятия, направленные на предотвращение, пресечение и ликвидацию последствий проведения террористических действий в информационном пространстве, а также наказание виновных в них лиц и организаций;

5) принимают необходимые меры законодательного и иного характера, которые гарантируют доступ законным образом на территорию государства-участника к отдельным частям информационно-коммуникационной инфраструктуры, в отношении которых имеются законные основания полагать их использование для ведения в информационном пространстве или с их использованием террористической деятельности или деятельности, способствующей проведению террористических актов или деятельности террористических организаций, групп или отдельных террористов.

#### **Глава 4. ОСНОВНЫЕ МЕРЫ ПРОТИВОДЕЙСТВИЯ ПРАВОНАРУШЕНИЯМ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ**

##### **Статья 10. Основные меры противодействия правонарушениям в информационном пространстве**

В целях противодействия правонарушениям в информационном пространстве государства-участники:

1) прилагают усилия по криминализации использования информационных ресурсов и (или) воздействия на них в информационном пространстве в противоправных целях, к которым в том числе относятся неправомерное распространение информации, нарушения конфиденциальности, целостности и доступности информации, а также принимают законодательные и иные меры, необходимые для того, чтобы установить и применить ответственность к лицам за покушение, соучастие, подстрекательство к совершению и совершение криминализированных социально опасных деяний в информационном пространстве;

2) принимают законодательные и иные меры, необходимые для того, чтобы к лицам, совершившим правонарушения в информационном пространстве, применялись эффективные, соразмерные и убедительные меры наказания.

##### **Статья 11. Меры по организации уголовного процесса**

В целях организации уголовного процесса государства-участники:

1) принимают законодательные и иные меры, необходимые для установления полномочий и процедур в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в

информационном пространстве криминализированных социально опасных деяний;

2) обеспечивают установление, исполнение и применение полномочий и процедур в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в информационном пространстве криминализированных социально опасных деяний в соответствии с условиями и гарантиями, предусмотренными его законодательством и обеспечивающими надлежащую защиту прав и свобод человека, и в соответствии с принципом соразмерности;

3) принимают законодательные и иные меры, необходимые для того, чтобы его компетентные органы имели возможность оперативно обеспечивать сохранность конкретных данных, включая данные о потоках информации, которые хранятся в информационно-коммуникационной инфраструктуре, когда имеются основания полагать, что эти данные особенно подвержены риску утраты или изменения;

4) принимают законодательные и иные меры, необходимые для того, чтобы гарантировать оперативное предоставление компетентным органам государства-участника или лицу, назначенному этими органами, достаточного количества данных о потоках информации, которые позволят идентифицировать поставщиков услуг и путь, которым передавалось конкретное сообщение в его информационном пространстве;

5) принимают законодательные и иные меры, которые могут потребоваться для предоставления его компетентным органам полномочий на обыск или иной аналогичный доступ к информационно-коммуникационным системам и их частям и хранящимся в них данным, носителям информации, на которых могут храниться искомые данные, на его территории, а также к другим данным и информационно-коммуникационным системам своего информационного пространства, в отношении которых имеется достаточно оснований полагать, что в них находятся искомые данные;

6) принимают законодательные и иные меры, необходимые для предоставления его компетентным органам полномочий требовать от лица, находящегося на территории государства и обладающего знаниями о функционировании соответствующей информационно-коммуникационной системы, применяемых мерах защиты, хранящихся там данных, для предоставления необходимых сведений, которые позволят им в пределах установленных полномочий осуществлять процедуры в целях проведения конкретных уголовных расследований или судебного разбирательства по фактам совершения в информационном пространстве криминализированных социально опасных деяний;

7) принимают законодательные и иные меры, необходимые для предоставления его компетентным органам полномочий собирать или записывать информацию с применением технических средств на его территории, а также обязать поставщиков услуг осуществлять в реальном масштабе времени аналогичные действия в сотрудничестве с компетентными органами данного государства;

8) принимают законодательные и иные меры для установления юрисдикции в отношении любого криминализованного социального опасного деяния в информационном пространстве, совершаемого на его территории, на борту судна, плавающего под флагом этого государства, на борту самолета или иного летательного аппарата, зарегистрированного согласно законам этого государства.

Если на юрисдикцию в отношении предполагаемого правонарушения претендует более одного государства-участника, заинтересованные государства проводят консультации с целью определения наиболее подходящей юрисдикции для осуществления судебного преследования.

## **Глава 5. МЕЖДУНАРОДНОЕ СОТРУДНИЧЕСТВО В СФЕРЕ МЕЖДУНАРОДНОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

### **Статья 12. Сотрудничество государств-участников**

1) Государства-участники обязуются осуществлять сотрудничество друг с другом в соответствии с положениями настоящей Конвенции и через применение других международных договоренностей.

2) Государства-участники на основе добровольности и взаимности обмениваются лучшими практиками в работе по предотвращению, правовому разбирательству и ликвидации последствий преступных деяний, включая действия в террористических целях, с использованием информационного пространства. Обмен может производиться как на двусторонней, так и на многосторонней основе. Государство-участник, предоставляющее информацию, вправе устанавливать требования о ее конфиденциальности. Государство-участник, получившее такую информацию, вправе использовать ее как аргумент в отношениях с предоставившим государством-участником при обсуждении вопросов взаимной помощи.

### **Статья 13. Меры доверия в области военного использования информационного пространства**

Каждое государство-участник должно стремиться к укреплению мер доверия в области военного использования информационного пространства, к которым относятся:

1) обмен национальными концепциями обеспечения безопасности в информационном пространстве;

2) оперативный обмен информацией о кризисных событиях и угрозах в информационном пространстве и принимаемых мерах в отношении их урегулирования и нейтрализации;

3) консультации по вопросам деятельности в информационном пространстве, которая может вызывать озабоченность государств-участников, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера.

#### **Статья 14. Консультативная помощь**

Государства-участники обязуются консультироваться и сотрудничать друг с другом в решении любых вопросов, которые могут возникнуть в отношении целей или в связи с выполнением положений настоящей Конвенции.

#### **ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ**

#### **Статья 15. Подписание Конвенции**

Настоящая Конвенция открыта для подписания ее всеми государствами.

#### **Статья 16. Ратификация Конвенции**

Настоящая Конвенция подлежит ратификации. Ратификационные грамоты сдаются на хранение Генеральному секретарю Организации Объединенных Наций.

#### **Статья 17. Присоединение к Конвенции**

Настоящая Конвенция открыта для присоединения к ней любого государства. Документы о присоединении сдаются на хранение Генеральному секретарю Организации Объединенных Наций.

#### **Статья 18. Вступление в силу Конвенции**

1. Настоящая Конвенция вступает в силу на тридцатый день после даты сдачи на хранение Генеральному секретарю Организации Объединенных Наций двадцатой ратификационной грамоты или документа о присоединении.
2. Для каждого государства, которое ратифицирует настоящую Конвенцию или присоединяется к ней после сдачи на хранение двадцатой ратификационной грамоты или документа о присоединении, настоящая Конвенция вступает в силу на тридцатый день после сдачи таким государством на хранение его ратификационной грамоты или документа о присоединении.

#### **Статья 19. Внесение поправок в Конвенцию**

1. Любое государство-участник может предложить поправку и представить ее Генеральному секретарю Организации Объединенных Наций. Генеральный секретарь затем препровождает предложенную поправку государствам-участникам с просьбой указать, высказываются ли они за созыв конференции государств-участников с целью рассмотрения этих предложений и проведения по ним голосования. Если в течение четырех месяцев, начиная с даты такого сообщения, по крайней мере одна треть государств-участников выскажется за такую конференцию, Генеральный секретарь созывает эту конференцию под эгидой Организации Объединенных Наций. Любая поправка, принятая большинством государств-участников, присутствующих и участвующих в голосовании на этой конференции, представляется Генеральной Ассамблее на утверждение.



2. Поправка, принятая в соответствии с пунктом 1 настоящей статьи, вступает в силу по утверждению ее Генеральной Ассамблеей Организации Объединенных Наций и принятия ее большинством в две трети государств-участников.

3. Когда поправка вступает в силу, она становится обязательной для тех государств-участников, которые ее приняли, а для других государств-участников остаются обязательными положения настоящей Конвенции и любые предшествующие поправки, которые ими приняты.

## **Статья 20. Оговорки к Конвенции**

1. Генеральный секретарь Организации Объединенных Наций получает и рассылает всем государствам текст оговорок, сделанных государствами в момент ратификации или присоединения.

2. Оговорка, не совместимая с целями и задачами настоящей Конвенции, не допускается.

3. Оговорки могут быть сняты в любое время путем соответствующего уведомления, направленного Генеральному секретарю Организации Объединенных Наций, который затем сообщает об этом всем государствам. Такое уведомление вступает в силу со дня его получения Генеральным секретарем.

## **Статья 21. Денонсация Конвенции**

Любое государство-участник может денонсировать настоящую Конвенцию путем письменного уведомления Генерального секретаря Организации Объединенных Наций. Денонсация вступает в силу по истечении одного года после получения уведомления Генеральным секретарем.

## **Статья 22. Депозитарий Конвенции**

Генеральный секретарь Организации Объединенных Наций назначается депозитарием настоящей Конвенции.

**Статья 23.** Подлинник настоящей Конвенции, английский, арабский, испанский, китайский, русский и французский тексты которой являются равно аутентичными, сдается на хранение Генеральному секретарю Организации Объединенных Наций.

В удостоверение чего нижеподписавшиеся полномочные представители, должным образом на то уполномоченные своими соответствующими правительствами, подписали настоящую Конвенцию.