

СОГЛАШЕНИЕ
о сотрудничестве государств – участников Содружества
Независимых Государств в области обеспечения
информационной безопасности

Правительства государств – участников Содружества Независимых Государств, далее именуемые Сторонами,

в целях осуществления взаимодействия при выполнении положений Концепции сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности, утвержденной Решением Совета глав государств СНГ от 10 октября 2008 года,

признавая важность совместного и эффективного использования новейших информационно-коммуникационных технологий для усиления противодействия угрозам информационной безопасности государств – участников СНГ,

учитывая, что дальнейшее развитие сотрудничества и взаимодействия Сторон в сфере обеспечения информационной безопасности является необходимостью и отвечает их интересам,

стремясь ограничить угрозы информационной безопасности государств – участников СНГ, обеспечить интересы государств в сфере информационной безопасности,

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

желая создать правовые и организационные основы сотрудничества государств – участников СНГ в сфере обеспечения информационной безопасности,

признавая необходимость предотвращения возможности использования информационно-коммуникационных технологий в целях, которые не совместимы с задачами обеспечения стабильности и безопасности государств – участников СНГ и способны оказать негативное воздействие на целостность инфраструктуры государств, нанося ущерб их безопасности как в гражданской, так и в военной сферах,

полагая, что для эффективной борьбы с правонарушениями в информационном обществе требуется более широкое, оперативное и хорошо отлаженное сотрудничество уполномоченных органов государств – участников СНГ,

согласились о нижеследующем:

Статья 1

Целью настоящего Соглашения является проведение совместных скоординированных мероприятий, направленных на обеспечение информационной безопасности в государствах – участниках настоящего Соглашения.

Статья 2

Для целей настоящего Соглашения приведенные термины имеют следующие значения:

воздействие на информацию – действие по изменению формы предоставления и/или содержания информации;

доступ к информации – возможность получения информации и ее использования;

защита информации – деятельность, направленная на защиту прав субъектов на информацию, предотвращение несанкционированного доступа к ней и/или утечки защищаемой информации, несанкционированных и/или непреднамеренных воздействий на нее;

защищаемая информация – информация, подлежащая защите в соответствии с законодательством государств – участников СНГ и/или требованиями, установленными обладателем данной информации;

информационная безопасность – состояние защищенности личности, общества и государства и их интересов от угроз, деструктивных и иных негативных воздействий в информационном пространстве;

информационная инфраструктура – совокупность технических средств и систем формирования, создания, преобразования, передачи, использования и хранения информации;

информационная преступность – использование информационных ресурсов и/или воздействие на них в информационном пространстве в противоправных целях;

информационная система – организационно упорядоченная совокупность средств, реализующих определенные технологические действия посредством информационных процессов, предназначенных для решения конкретных функциональных задач;

информационное оружие – информационные технологии, средства и методы, применяемые в целях 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 – информационные процессы и методы работы с информацией, осуществляемые с применением средств вычислительной техники и средств телекоммуникации;

информационные процессы – процессы формирования, поиска, сбора, обработки, хранения, распространения и использования информации;

информационные ресурсы – информационная инфраструктура, а также собственно информация и ее потоки;

информационные технологии – совокупность методов, производственных процессов и программно-технических средств, объединенных в технологический комплекс, обеспечивающий сбор, создание, хранение, накопление, обработку, поиск, вывод, копирование, передачу, распространение и защиту информации;

информационный терроризм – использование информационных ресурсов и/или воздействие на них в информационном пространстве в террористических целях;

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

информация ограниченного доступа – информация, доступ к которой ограничен законодательством государств – участников СНГ либо их международными договорами;

межгосударственная информационная система – задействованная в межгосударственных информационных обменах система, принадлежащая органам СНГ, субъектам государств – участников СНГ на правах совместной собственности, совместного владения или совместного (общего) пользования;

несанкционированный доступ к информации – доступ к защищаемой информации с нарушением прав или правил, установленных ее обладателем, владельцем и/или законодательством государств – участников СНГ;

обеспечение информационной безопасности – система мер правового, организационно-технического и организационно-экономического характера по выявлению угроз информационной безопасности, предотвращению их реализации, пресечению и ликвидации последствий реализации таких угроз;

сертификация на соответствие требованиям по защите информации – форма подтверждения соответствия объектов оценки требованиям по защите информации, установленным в нормативных правовых актах государств – участников настоящего Соглашения;

средство защиты информации – техническое, программное, программно-техническое средство, вещество и/или материал, предназначенный или используемый для защиты информации;

трансграничная передача информации – передача информации оператором через государственные границы государств – участников СНГ органу власти, физическому или юридическому лицу государства;

угрозы информационной безопасности – факторы, создающие опасность для личности, общества, государства и их интересов в информационном пространстве.

В целях настоящего Соглашения под угрозами информационной безопасности понимаются в том числе разработка и применение информационного оружия, информационный терроризм и информационная преступность;

уполномоченные органы – органы Сторон, наделенные соответствующей компетенцией и полномочиями, осуществляющие координацию деятельности в сфере информационной безопасности.

Статья 3

Стороны организуют взаимодействие и сотрудничество по следующим основным направлениям:

сближение нормативных правовых актов и нормативно-методических документов государств – участников настоящего Соглашения, регламентирующих отношения в сфере обеспечения информационной безопасности;

разработка нормативных правовых актов для проведения совместных скоординированных мероприятий в информационном пространстве, направленных на обеспечение информационной безопасности в государствах – участниках настоящего Соглашения;

разработка и доведение до пользователей нормативных документов, регулирующих вопросы обеспечения информационной безопасности;

нормативное правовое обеспечение развития производства программно-технических средств и средств защиты информации;

разработка межгосударственных стандартов в области информационной безопасности, совместимых с международными стандартами;

создание защищенных информационных систем различного прикладного назначения;

организация трансграничной передачи информации;

совершенствование технологии защиты информационных систем и ресурсов от потенциальных и реальных угроз;

анализ и оценка угроз информационной безопасности информационных систем;

совершенствование деятельности в области выявления и нейтрализации устройств и программ, представляющих опасность для функционирования информационных систем;

реализация согласованных мероприятий, направленных на недопущение несанкционированного доступа к информации, размещенной в информационных системах, и ее утечки по техническим каналам;

обеспечение защиты информации ограниченного доступа и информационных технологий при взаимодействии информационных систем различных классов защищенности;

модернизация принадлежащих государствам – участникам настоящего Соглашения сегментов межгосударственных информационных систем и их программного обеспечения;

установление согласованного порядка сертификации и взаимного признания результатов сертификации средств защиты информации;

разработка перспективных информационных технологий в области информационной безопасности;

экспертиза научно-исследовательских и опытно-конструкторских работ, научно-технической продукции в области информационной безопасности;

профессиональная переподготовка и повышение квалификации кадров в области обеспечения информационной безопасности;

обобщение, распространение и внедрение передового опыта;

организация и проведение научных конференций, симпозиумов и совещаний.

Статья 4

Стороны предпринимают консолидированные усилия по противодействию угрозам использования информационно-коммуникационных средств и технологий в целях совершения противоправных и иных деструктивных действий как в мирное время, так и в угрожаемый период в отношении государств – участников СНГ.

Стороны разрабатывают и реализуют межгосударственные программы, обеспечивающие комплексное решение вопросов информационной безопасности, и отдельные проекты по реализации представляющих взаимный интерес конкретных направлений сотрудничества.

Стороны в соответствии с законодательством государств – участников настоящего Соглашения стремятся к упрощению порядка обмена данными о работах, проводимых в области обеспечения информационной безопасности.

Стороны создают условия для активного участия государственных органов и организаций, независимо от форм собственности, в работах по обеспечению информационной безопасности.

Стороны проводят совместные мероприятия по вопросам обеспечения информационной безопасности на принципах равноправия и взаимной выгоды.

Стороны проводят консультации на основе настоящего Соглашения в целях координации и повышения эффективности сотрудничества.

Статья 5

Стороны осуществляют меры, предусматривающие проведение работ по реализации настоящего Соглашения поэтапно.

На первом этапе Стороны обеспечивают сбор, анализ и обмен информацией, необходимой для реализации направлений сотрудничества, указанных в статье 3 настоящего Соглашения, разрабатывают и доводят до уполномоченных органов других Сторон нормативные правовые акты, регулирующие вопросы обеспечения информационной безопасности.

Стороны принимают согласованные меры к упрощению порядка обмена информацией о работах, проводимых в области информационной безопасности.

На последующих этапах Стороны организуют реализацию направлений сотрудничества, указанных в статье 3 настоящего Соглашения, в согласованные сроки.

Статья 6

Стороны обязуются не разглашать и обеспечить надлежащей защитой информацию ограниченного доступа, которая стала известна им в процессе реализации настоящего Соглашения.

В рамках настоящего Соглашения не осуществляется передача сведений, отнесенных законодательством государств – участников настоящего Соглашения к государственной тайне (государственным секретам).

Статья 7

Стороны самостоятельно несут расходы, возникающие в ходе реализации ими положений настоящего Соглашения, если в каждом конкретном случае не будет согласован иной порядок.

Статья 8

Ответственными за реализацию настоящего Соглашения являются уполномоченные органы, перечень которых определяется каждой Стороной и передается депозитарию при сдаче уведомления о выполнении внутригосударственных процедур, необходимых для вступления настоящего Соглашения в силу, или документа о присоединении.

Каждая из Сторон в течение 30 дней письменно уведомляет депозитарий об изменениях перечня уполномоченных органов.

Статья 9

Уполномоченные органы обмениваются между собой информацией по основным направлениям взаимодействия и сотрудничества, приведенным в статье 3 настоящего Соглашения.

Уполномоченные органы осуществляют обмен опытом между Сторонами по вопросам обеспечения информационной безопасности и других информационных технологий, а также средств защиты информации.

Статья 10

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон, вытекающих для нее из других международных договоров, участником которых является ее государство.

Статья 11

В настоящее Соглашение по взаимному согласию Сторон могут быть внесены изменения и дополнения, являющиеся его неотъемлемой частью, которые оформляются соответствующим протоколом.

Статья 12

Спорные вопросы между Сторонами, возникающие при применении и толковании настоящего Соглашения, решаются путем консультаций и переговоров заинтересованных Сторон.

Статья 13

Настоящее Соглашение вступает в силу по истечении 30 дней с даты получения депозитарием третьего уведомления о выполнении подписавшими его Сторонами внутригосударственных процедур, необходимых для его вступления в силу.

Для Сторон, выполнивших внутригосударственные процедуры позднее, настоящее Соглашение вступает в силу по истечении 30 дней с даты получения депозитарием соответствующих документов.

Статья 14

Настоящее Соглашение после его вступления в силу открыто для присоединения любого государства – участника СНГ путем передачи депозитарию документа о присоединении.

Для присоединяющегося государства настоящее Соглашение вступает в силу по истечении 30 дней с даты получения депозитарием документа о присоединении.

Статья 15

Настоящее Соглашение заключается на неопределенный срок. Каждая из Сторон вправе выйти из настоящего Соглашения, направив депозитарию письменное уведомление о таком своем намерении не позднее чем за 6 месяцев до выхода и урегулировав обязательства, возникшие за время действия настоящего Соглашения.

Совершено в городе Санкт-Петербурге 20 ноября 2013 года в одном подлинном экземпляре на русском языке. Подлинный экземпляр хранится в Исполнительном комитете Содружества Независимых Государств, который направит каждому государству, подписавшему настоящее Соглашение, его заверенную копию.

За Правительство
Азербайджанской Республики

За Правительство
Республики Армения

За Правительство
Республики Беларусь

За Правительство
Республики Казахстан

За Правительство
Кыргызской Республики

За Правительство
Республики Молдова

За Правительство
Российской Федерации

За Правительство
Республики Таджикистан

За Правительство
Туркменистана

За Правительство
Республики Узбекистан

За Правительство
Украины