О подписании Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности

Постановление Правительства Республики Казахстан от 12 июня 2009 года № 902

Правительство Республики Казахстан **ПОСТАНОВЛЯЕТ** :

1. Одобрить прилагаемый проект Соглашения между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.

2. Уполномочить Министра иностранных дел Республики Казахстан Тажина Марата Муханбетказиевича подписать от имени Правительства Республики Казахстан Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности, разрешив вносить изменения и дополнения, не имеющие принципиального характера.

3. Настоящее постановление вводится в действие со дня подписания.

Премьер-Министр

Республики Казахстан *К. Масимов*

Проект

Одобрено
постановлением Правительства
Республики Казахстан
от 12 июня 2009 года № 902

СОГЛАШЕНИЕ
между правительствами государств-членов
Шанхайской организации сотрудничества
о сотрудничестве в области обеспечения
международной информационной безопасности

Правительства государств-членов Шанхайской организации сотрудничества (ШОС), далее именуемые Стороны,

отмечая значительный прогресс в развитии и внедрении новейших информационно-коммуникационных технологий и средств, формирующих глобальное информационное пространство,

выражая озабоченность угрозами, связанными с возможностями использования

таких технологий и средств в целях, не совместимых с задачами обеспечения международной стабильности и безопасности, применительно как к гражданской, так и к военной сферам,

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 Сторон в вопросах обеспечения международной информационной безопасности является настоятельной необходимостью и отвечает их интересам,

принимая также во внимание важную роль информационной безопасности в обеспечении прав и основных свобод человека и гражданина,

учитывая рекомендации резолюций Генеральной Ассамблеи ООН "Достижения в сфере информатизации и телекоммуникаций в контексте международной безопасности",

стремясь ограничить угрозы международной информационной безопасности, обеспечить интересы информационной безопасности Сторон и создать международную информационную среду, для которой характерны мир, сотрудничество и гармония,

желая создать правовые и организационные основы сотрудничества Сторон в области обеспечения международной информационной безопасности,

согласились о нижеследующем:

Статья 1. Термины и понятия

Для целей взаимодействия Сторон в рамках выполнения настоящего Соглашения будет использоваться Перечень основных терминов и понятий в области обеспечения международной информационной безопасности согласно приложению 1 к настоящему Соглашению, являющемуся его неотъемлемой частью.

Содержание данного перечня терминов и понятий может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 2. Основные угрозы в области обеспечения международной информационной безопасности

Реализуя сотрудничество в соответствии с настоящим Соглашением Стороны исходят из наличия следующих основных угроз в области обеспечения международной информационной безопасности:

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

2. Информационный терроризм.

3. Информационная преступность.

4. Использование доминирующего положения в информационном пространстве в

ущерб интересам и безопасности других государств.

5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

6. Угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и/или техногенный характер.

Согласованное понимание Сторонами существа перечисленных основных угроз приведено в Перечне видов угроз в области международной информационной безопасности, их источников и признаков, согласно приложению 2 к настоящему Соглашению, являющемуся его неотъемлемой частью.

Содержание данного Перечня может по мере необходимости дополняться, уточняться и обновляться по согласованию Сторон.

Статья 3. Основные направления сотрудничества

С учетом угроз, изложенных в Статье 2 настоящего Соглашения, Стороны, их уполномоченные представители, а также национальные компетентные органы, которые определяются в соответствии со Статьей 5 настоящего Соглашения, осуществляют сотрудничество в области обеспечения международной информационной безопасности по следующим основным направлениям:

1. Определение, согласование и осуществление необходимых совместных мер в области обеспечения международной информационной безопасности.

2. Создание системы мониторинга и совместного реагирования на возникающие в данной области угрозы.

3. Выработка совместных мер по развитию норм международного права в области ограничения распространения и применения информационного оружия, создающего угрозы обороноспособности, национальной и общественной безопасности.

4. Противодействие угрозам использования информационно-коммуникационных технологий в террористических целях.

5. Противодействие информационной преступности.

6. Проведение необходимых для целей настоящего Соглашения экспертиз, исследований и оценок в области обеспечения информационной безопасности.

7. Содействие обеспечению безопасного, стабильного функционирования и интернационализации управления глобальной сетью Интернет.

8. Обеспечение информационной безопасности национальных критически важных структур.

9. Разработка и осуществление совместных мер доверия, способствующих обеспечению международной информационной безопасности.

10. Разработка и осуществление согласованной политики и организационно-технических процедур по реализации возможностей использования электронной цифровой подписи и защиты информации при трансграничном информационном обмене.

11. Обмен информацией о национальном законодательстве по вопросам обеспечения информационной безопасности.

12. Совершенствование международно-правовой базы и практических механизмов сотрудничества Сторон в обеспечении международной информационной безопасности.

13. Создание условий для взаимодействия национальных компетентных органов в целях реализации настоящего Соглашения.

14. Координация позиций в рамках международных организаций и форумов по проблемам обеспечения международной информационной безопасности.

15. Обмен опытом, подготовка специалистов, проведение рабочих встреч, конференций, семинаров и других форумов уполномоченных представителей и экспертов Сторон в области информационной безопасности.

16. Обмен информацией по вопросам, связанным с осуществлением сотрудничества по перечисленным в настоящей Статье основным направлениям.

Стороны или национальные компетентные органы могут по взаимной договоренности определять другие направления сотрудничества.

Статья 4. Общие принципы сотрудничества

1. Стороны осуществляют сотрудничество и свою деятельность в международном информационном пространстве в рамках настоящего Соглашения таким образом, чтобы такая деятельность способствовала социальному и экономическому развитию и была совместимой с задачами поддержания международной стабильности и безопасности, 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, а также принципам регионального сотрудничества и невмешательства в национальные информационные ресурсы.

2. Деятельность Сторон в рамках настоящего Соглашения должна быть совместимой с правом каждой Стороны искать, получать и распространять информацию, с учетом того, что такое право может быть ограничено законодательством в целях защиты интересов национальной и общественной безопасности.

3. Каждая Сторона имеет равное право на защиту своих национальных информационных ресурсов и критически важных структур от неправомерного

использования и несанкционированного вмешательства, в том числе от информационных атак на них.

Каждая Сторона не будет проводить по отношению к другой Стороне подобных действий, и будет оказывать содействие другим Сторонам в реализации вышеуказанного права.

Статья 5. Основные формы и механизмы сотрудничества

1. В течение шестидесяти дней с даты вступления настоящего Соглашения в силу Стороны взаимно обменяются через Депозитария данными о национальных компетентных органах, ответственных за реализацию настоящего Соглашения, и каналах прямого обмена информацией по конкретным направлениям сотрудничества.

2. С целью рассмотрения хода выполнения настоящего Соглашения, обмена информацией, анализа и совместной оценки возникающих угроз информационной безопасности, а также определения, согласования и координации совместных мер реагирования на такие угрозы, Стороны будут проводить на регулярной основе консультации уполномоченных представителей Сторон и национальных компетентных органов (далее - консультации).

Очередные консультации будут проводиться по согласованию Сторон, как правило, раз в полугодие в Секретариате ШОС или на территории государства одной из Сторон по ее приглашению.

Любая из Сторон может инициировать проведение внеочередных консультаций, предлагая время и место, а также повестку дня для последующего согласования со всеми Сторонами и Секретариатом ШОС.

3. Практическое взаимодействие по конкретным направлениям сотрудничества, предусмотренным настоящим Соглашением, Стороны могут осуществлять по линии национальных компетентных органов, ответственных за реализацию Соглашения.

4. В целях создания правовых и организационных основ сотрудничества по конкретным направлениям национальные компетентные органы могут заключать соответствующие договоры межведомственного характера.

Статья 6. Защита информации

1. Настоящее Соглашение не налагает на Стороны обязательств по предоставлению информации в рамках сотрудничества и не является основанием для передачи информации в рамках сотрудничества, если раскрытие такой информации может нанести ущерб национальным интересам.

2. В рамках сотрудничества в соответствии с настоящим Соглашением Стороны не осуществляют обмен информацией, которая согласно национальному законодательству любой из Сторон относится к государственной тайне и/или государственным секретам.

Порядок передачи и обращения с подобной информацией, которая в конкретных случаях может считаться необходимой для целей исполнения настоящего Соглашения, регулируется на основании и на условиях соответствующих договоров между Сторонами.

3. Стороны обеспечивают надлежащую защиту передаваемой или создаваемой в ходе сотрудничества в рамках настоящего Соглашения информации, не относящейся по национальному законодательству любой из Сторон к государственной тайне и/или государственным секретам, доступ к которой и распространение которой ограничены в соответствии с национальным законодательством и/или соответствующими нормативными актами любой из Сторон.

Защита такой информации осуществляется в соответствии с национальным законодательством и/или соответствующими нормативными актами получающей Стороны. Такая информация не раскрывается и не передается без письменного согласия Стороны - первичного источника этой информации.

Такая информация должным образом обозначается в соответствии с национальным законодательством и/или соответствующими нормативными актами Сторон.

Статья 7. Финансирование

Стороны самостоятельно несут расходы по участию их представителей и экспертов в соответствующих мероприятиях по исполнению настоящего Соглашения.

По прочим расходам, связанным с исполнением настоящего Соглашения, Стороны в каждом отдельном случае могут согласовывать иной порядок финансирования в соответствии с национальным законодательством.

Статья 8. Отношение к другим международным договорам

Настоящее Соглашение не затрагивает прав и обязательств каждой из Сторон по другим международным договорам, участником которых является ее государство.

Статья 9. Разрешение споров

Стороны решают спорные вопросы, которые могут возникнуть в связи с толкованием или применением положений настоящего Соглашения, путем консультаций и переговоров.

Статья 10. Рабочие языки

Рабочими языками при осуществлении сотрудничества в рамках настоящего Соглашения являются русский и китайский языки.

Статья 11. Депозитарий

Депозитарием настоящего Соглашения является Секретариат ШОС.

Подлинный экземпляр настоящего Соглашения хранится у Депозитария, который в течение пятнадцати дней, начиная с даты его подписания, направит Сторонам его заверенные копии.

Статья 12. Заключительные положения

1. Настоящее Соглашение заключается на неопределенный срок и вступает в силу на тридцатый день с даты получения Депозитарием четвертого уведомления в письменной форме о выполнении Сторонами внутригосударственных процедур, необходимых для вступления в силу настоящего Соглашения. Для Стороны, выполнившей внутригосударственные процедуры позднее, настоящее Соглашение вступает в силу на тридцатый день с даты получения Депозитарием ее соответствующего уведомления.

2. По взаимному согласию Стороны могут предлагать дополнения и изменения в Соглашение, которые оформляются отдельным протоколом.

3. Настоящее Соглашение не направлено против каких-либо государств и организаций и после его вступления в силу открыто для присоединения любого государства, разделяющего цели и принципы настоящего Соглашения, путем передачи Депозитарию документа о присоединении. Для присоединившегося государства настоящее Соглашение вступает в силу по истечении тридцати дней с даты получения Депозитарием последнего уведомления о согласии подписавших его и присоединившихся к нему государств на такое присоединение.

4. Каждая из Сторон может выйти из настоящего Соглашения, направив Депозитарию письменное уведомление об этом не менее чем за девяносто дней до предполагаемой даты выхода. Депозитарий извещает о данном намерении другие Стороны в течение тридцати дней с даты получения им уведомления Стороны о выходе из Соглашения.

5. В случае прекращения действия настоящего Соглашения Стороны принимают меры к полному выполнению обязательств по защите информации, а также ранее согласованных совместных работ, проектов и иных мероприятий, осуществляемых в рамках Соглашения и не завершенных к моменту прекращения действия Соглашения.

Совершено в городе _____ _____ 2009 года в одном подлинном экземпляре на русском и китайском языках, причем оба текста имеют одинаковую силу.

За Правительство

Республики Казахстан

За Правительство Китайской Народной Республики

За Правительство Кыргызской Республики

За Правительство Российской Федерации

За Правительство Республики Таджикистан

За Правительство Республики Узбекистан

Приложение 1
к Соглашению
между правительствами государств-членов
Шанхайской организации сотрудничества
о сотрудничестве в области обеспечения
международной информационной безопасности

Перечень
основных терминов и понятий
в области обеспечения международной информационной безопасности

Информационная безопасность - состояние защищенности личности, общества и государства и их интересов 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, массированной 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, создания, преобразования, передачи, использования и хранения информации.

Информационное оружие - информационные технологии, средства и методы, применяемые в целях ведения информационной войны.

Информационная преступность - использование информационных ресурсов и/или воздействие на них в информационном пространстве в противоправных целях.

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.

Информационные ресурсы - информационная инфраструктура, а также собственно информация и ее потоки.

Информационный терроризм - использование информационных ресурсов и/или воздействие на них в информационном пространстве в террористических целях.

Критически важные структуры - объекты, системы и институты государства, воздействие на которые может иметь последствия, прямо 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, национального законодательства или норм международного права.

Несанкционированное вмешательство в информационные ресурсы - неправомерное воздействие на процессы формирования, создания, обработки, преобразования, передачи, использования, хранения информации.

Угроза информационной безопасности - факторы, создающие опасность личности, обществу, государству и их интересам в информационном пространстве.

Приложение 2
к Соглашению
между правительствами государств-членов
Шанхайской организации сотрудничества
о сотрудничестве в области обеспечения
международной информационной безопасности

Перечень
видов угроз в области международной информационной безопасности, их источников и признаков

1. Разработка и применение информационного оружия, подготовка и ведение информационной войны.

Источником угрозы является создание и развитие информационного оружия, представляющего непосредственную угрозу для критически важных структур государств, что может привести к новой гонке вооружений и представляет главную угрозу в области международной информационной безопасности.

Ее признаками являются: применение информационного оружия в целях подготовки и ведения информационной войны, а также воздействия на системы транспортировки, коммуникаций и управления воздушными, противоракетными и другими видами объектов обороны, в результате чего государство утрачивает способность обороняться перед лицом агрессора и не может воспользоваться законным правом самозащиты; нарушение функционирования объектов информационной инфраструктуры, в результате чего парализуются системы управления и принятия решений в государствах, деструктивное воздействие на критически важные структуры.

2. Информационный терроризм.

Источником угрозы являются террористические организации и лица, причастные к террористической деятельности, осуществляющие свои противоправные действия посредством или в отношении информационных ресурсов.

Ее признаками являются: использование информационных сетей террористическими организациями для осуществления террористической деятельности и привлечения в свои ряды новых сторонников; деструктивное воздействие на информационные ресурсы, приводящие к нарушению общественного порядка; контролирование или блокирование каналов передачи массовой информации; использование Интернета или других информационных сетей для пропаганды терроризма, создания атмосферы страха и паники в обществе, а также иные негативные воздействия на информационные ресурсы.

3. Информационная преступность.

Источником угрозы являются лица или организации, осуществляющие неправомерное использование информационных ресурсов или несанкционированное вмешательство в такие ресурсы в преступных целях.

Ее признаками являются: проникновение в информационные системы для нарушения целостности, доступности и конфиденциальности информации; умышленное изготовление и распространение компьютерных вирусов и других вредоносных программ; осуществление DOS-атак (denial of service) и иных негативных воздействий; причинение ущерба информационным ресурсам; нарушение законных прав и свобод граждан в информационной сфере, в том числе права интеллектуальной собственности и неприкосновенности частной жизни; использование информационных ресурсов и методов для совершения таких преступлений, как мошенничество, хищение, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и т.д.

4. Использование доминирующего положения в информационном пространстве в ущерб интересам и безопасности других стран.

Источником угрозы является неравномерность в развитии информационных технологий в различных государствах и существующая тенденция к увеличению " цифрового разрыва" между развитыми и развивающимися странами. Некоторые

государства, имеющие преимущества в развитии информационных технологий, умышленно ограничивают развитие прочих стран и получение доступа к информационным технологиям, что приводит к возникновению серьезной опасности для государств с недостаточными информационными возможностями.

Ее признаками являются: монополизация производства программного обеспечения и оборудования информационных инфраструктур, ограничение участия государств в международном информационно-технологическом сотрудничестве, препятствующее их развитию и увеличивающее зависимость этих стран от более развитых государств. Встраивание скрытых возможностей и функций в программное обеспечение и оборудование, поставляемые в другие страны, для контроля и влияния на информационные ресурсы и/или критически важные структуры этих стран. Контроль и монополизация рынка информационных технологий и продуктов в ущерб интересам и безопасности государств.

5. Распространение информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Источником угрозы являются государства, организации, группа лиц или частное лицо использующие информационную инфраструктуру для распространения информации, наносящей вред общественно-политической и социально-экономической системам, духовной, нравственной и культурной среде других государств.

Ее признаками являются появление и тиражирование в электронных (радио и телевидение) и прочих средствах массовой информации, в Интернете и других сетях информационного обмена информации:

искажающей представление о политической системе, общественном строе, внешней и внутренней политике, важных политических и общественных процессах в государстве, духовных, нравственных и культурных ценностях его населения;

пропагандирующей идеи терроризма, сепаратизма и экстремизма;

разжигающей межнациональную, межрасовую и межконфессиональную вражду.

6. Угрозы безопасному, стабильному функционированию глобальных и национальных информационных инфраструктур, имеющие природный и/или техногенный характер.

Источниками угроз являются стихийные бедствия и другие опасные природные явления, а также катастрофы техногенного характера, возникающие внезапно или в результате длительного процесса, способные оказать масштабное разрушительное воздействие на информационные ресурсы государства.

Ее признаками являются: нарушение функционирования объектов информационной инфраструктуры и, как следствие, дестабилизация критически важных структур, государственных систем управления и принятия решений, результаты которой прямо затрагивают безопасность государства и общества.

© 2012. РГП на ПХВ «Институт законодательства и правовой информации Республики Казахстан»
Министерства юстиции Республики Казахстан