О Концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере

Решение Совета глав правительств Содружества Независимых Государств от 4 июня 1999 года

Совет глав правительств Содружества,

руководствуясь Соглашением о взаимном обеспечении сохранности межгосударственных секретов от 22 января 1993 года,

в соответствии с Решением Совета глав государств Содружества Независимых Государств от 28 марта 1997 года об Основных мероприятиях интеграционного развития государств-участников Содружества Независимых Государств на 1997 год **решил** :

1. Утвердить Концепцию информационной безопасности государств-участников Содружества Независимых Государств в военной сфере (прилагается).

2. Определить Концепцию информационной безопасности государств-участников Содружества Независимых Государств в военной сфере как основу для разработки документов об обеспечении информационной безопасности государств-участников СНГ в военной сфере.

3. Настоящее Решение вступает в силу со дня его подписания.

Совершено в городе Минске 4 июня 1999 года в одном подлинном экземпляре на русском языке. Подлинный экземпляр хранится в Исполнительном комитете Содружества Независимых Государств, который направит каждому государству, подписавшему настоящее Решение, его заверенную копию.

За Правительство Республики Армения	*За Правительство Кыргызской Республики*
За Правительство Республики Беларусь	*За Правительство Российской Федерации*
За Правительство Республики Казахстан	*За Правительство Республики Таджикистан*

Решение подписано Республикой Беларусь с замечанием: "Решение Совета глав правительств СНГ о Концепции информационной безопасности государств-участников Содружества Независимых Государств в военной сфере для Республики Беларусь будет действовать в следующей редакции:

"Одобрить проект Концепции информационной безопасности

государств-участников Содружества Независимых Государств в военной сфере и внести его на рассмотрение Совета глав государств".

14.07.99 г. МИД Республики Беларусь уведомил депозитарий о том, что "замечание Республики Беларусь следует рассматривать в качестве заявления, которое не влияет на обязательность вышеупомянутого Решения для Республики Беларусь и действие Концепции в отношении Республики Беларусь".

Решение не подписано Азербайджанской Республикой, Грузией, Республикой Молдова, Туркменистаном, Республикой Узбекистан, Украиной.

Утверждена
Решением Совета глав правительств
Содружества Независимых Государств о
Концепции информационной безопасности
государств-участников Содружества
Независимых Государств в военной сфере

4 июня 1999 года

КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В ВОЕННОЙ СФЕРЕ

Концепция информационной безопасности государств-участников Содружества Независимых Государств в военной сфере (далее - Концепция) разработана на основе Соглашения о взаимном обеспечении сохранности межгосударственных секретов от 22 января 1993 года.

Настоящая Концепция представляет собой официально принятую государствами-участниками Содружества систему взглядов на цели, задачи и принципы обеспечения информационной безопасности в военной сфере. В ней определены объекты информационной безопасности в военной сфере, возможные источники угрозы, методы предотвращения и нейтрализации этих угроз, а также основы согласованной политики в области информационной безопасности в военной сфере.

I. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Назначение Концепции:

Концепция является основой для формирования межгосударственной информационной политики, единого информационного пространства, разработки и проведения мероприятий по обеспечению информационной безопасности в военной сфере государств-участников Содружества.

Положения Концепции необходимо учитывать при:

формировании и реализации собственной государственной политики в области информационной безопасности;

разработке и совершенствовании методического, научно-технического и организационного обеспечения информационной безопасности, а также целевых программ обеспечения информационной безопасности при решении совместных задач обороны;

использовании вооружения и военной техники другого государства и совместных научно-технических разработках в области обороны.

1.2. Цель и основные задачи обеспечения информационной безопасности государств-участников Содружества Независимых Государств в военной сфере.

Целью обеспечения информационной безопасности государств-участников Содружества в военной сфере является защита информационной среды, информационного потенциала и информационных технологий, составляющих межгосударственные секреты или конфиденциальную информацию, переданную в совместное пользование.

Цель обеспечения информационной безопасности в военной сфере определяется общими и национальными интересами государств-участников Содружества. При этом государства-участники Содружества берут на себя обязательства:

соблюдения прав государств-участников Содружества в области информации;

надежной защиты переданных в совместное пользование сведений, составляющих межгосударственные секреты или конфиденциальную информацию;

совместного развития производства средств информатизации, телекоммуникации и связи, используемых в интересах коллективной обороны.

К основным задачам обеспечения информационной безопасности государств-участников Содружества в военной сфере относятся:

определение совместных интересов в информационной сфере;

совершенствование и согласование нормативно-правовой базы обеспечения информационной безопасности при решении совместных задач в интересах коллективной обороны;

обеспечение безопасности информационных и телекоммуникационных систем, как развернутых, так и создаваемых в интересах коллективной безопасности;

выявление, оценка и прогнозирование угроз информационной безопасности;

координация деятельности органов государственной власти, предприятий, учреждений и организаций (далее - предприятия) независимо от форм собственности в области обеспечения информационной безопасности при решении задач коллективной обороны;

совместное развитие систем и средств обеспечения информационной безопасности, используемых в интересах коллективной обороны;

совершенствование методов предотвращения и нейтрализации угроз информационной безопасности;

организация антивирусной защиты информационного потенциала и сертификация

информационных процессов, изделий и программ, предназначенных для решения задач коллективной обороны и безопасности, по требованиям информационной безопасности ;

лицензирование деятельности предприятий по проведению работ, связанных с использованием сведений, составляющих межгосударственные секреты, а также с созданием средств защиты информации и осуществлением мероприятий по оказанию услуг по защите межгосударственных секретов в соответствии с законодательством, действующим на территории данного государства;

защита информации от утечки по каналам связи;

регламентация порядка и правил использования технических средств передачи и обработки информации, предназначенных для решения задач коллективной обороны и безопасности.

1.3. Основные принципы обеспечения информационной безопасности государств-участников Содружества Независимых Государств в военной сфере.

Для реализации целей и задач обеспечения информационной безопасности в военной сфере государства-участники Содружества руководствуются принципами:

согласованности приоритетов государственных политик в области обеспечения информационной безопасности в военной сфере;

координации разработки и реализации государственных нормативно-правовых документов о вопросах информационной безопасности в военной сфере;

опережающего развития нормативно-правовой базы, регламентирующей информационные отношения, в том числе в области информационной безопасности в военной сфере;

поддержки отечественных производителей в области информационных технологий и производителей других государств-участников Содружества;

непрерывности обеспечения меры информационной безопасности при использовании национальных и коллективных систем телекоммуникации, связи и управления войсками и оружием;

неукоснительности соблюдения единых методов предотвращения и нейтрализации угроз безопасности в информационной сфере;

полного исключения несанкционированного доступа к информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации или сбои в работе средств информатизации.

II. ИСТОЧНИКИ УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В ВОЕННОЙ СФЕРЕ

Источниками угроз информационной безопасности государств-участников Содружества в военной сфере являются:

государственная политика ряда зарубежных стран, направленная на осуществление

глобального мониторинга политических, экономических, военных, экологических и других процессов в целях получения односторонних преимуществ;

все виды разведывательной деятельности зарубежных государств, а также радиоэлектронные и технические воздействия со стороны иностранных государств;

нарушение установленных регламентов сбора, обработки и передачи информации;

преднамеренные и непреднамеренные ошибки персонала информационных систем, систем и средств управления военного назначения;

внедрение программ-вирусов и программных закладок в общее и прикладное программное обеспечение и средства защиты информации в военной сфере;

низкий уровень информационных технологий, ориентация на широкое использование импортного технического и программного обеспечения, а также расширение участия зарубежных компаний в развитии информационной инфраструктуры государств-участников Содружества;

отсутствие необходимой нормативно-правовой базы, регулирующей межгосударственные отношения в информационной сфере, в том числе в области обеспечения информационной безопасности в военной сфере;

обострение криминогенной обстановки, возрастание масштабов компьютерной преступности;

отсутствие единой политики и необходимой инфраструктуры в информационной сфере;

использование для решения задач коллективной безопасности информационных и телекоммуникационных систем, создающих условия для утечки информации, составляющей межгосударственные секреты, а также конфиденциальной информации;

использование не сертифицированных по требованиям безопасности информации программных средств и средств защиты информации в военной сфере.

Эти источники угроз будут представлять особую опасность в условиях обострения военно-политической обстановки.

III. ОБЪЕКТЫ И МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В ВОЕННОЙ СФЕРЕ

3.1. Объекты обеспечения информационной безопасности.

Под объектами обеспечения информационной безопасности понимаются объекты, на которых необходимо предусматривать меры предотвращения или ликвидации угроз в информационной сфере, используя принципы и методы, изложенные в настоящей Концепции, и другие, принятые государством-участником Содружества. К ним относятся:

информационные системы, системы и средства управления войсками и оружием;

информационные процессы, информационные ресурсы и информационная

инфраструктура, используемые в военной сфере;

система формирования, распространения и использования информационных процессов, используемых в военной сфере;

информационные технологии военного и двойного назначения, системы и средства защиты информации, используемые в военной сфере;

предприятия и научно-исследовательские организации, выполняющие оборонные заказы, либо занимающиеся оборонной проблематикой в интересах государств-участников Содружества;

вооружение, военная техника и военные объекты, имеющие охраняемые параметры (характеристики).

3.2. Методы обеспечения информационной безопасности государств-участников Содружества Независимых Государств в военной сфере.

Для предотвращения и нейтрализации угроз информационной безопасности применяются правовые, организационные и программно-технические методы.

Правовые методы предусматривают разработку согласованных нормативно-правовых актов, регламентирующих информационные отношения между государствами-участниками Содружества по обеспечению их информационной безопасности.

Организационные методы предусматривают:

согласованное формирование и обеспечение функционирования систем защиты информации в военной сфере;

сертификацию этих систем по требованиям информационной безопасности в соответствии с законодательством, действующим на территории данного государства;

лицензирование деятельности предприятий по проведению работ, связанных с использованием сведений, составляющих межгосударственные секреты, в соответствии с законодательством, действующим на территории данного государства;

создание средств защиты информации, а также осуществление мероприятий и оказание услуг по защите межгосударственных секретов;

стандартизацию способов и средств защиты информации;

контроль соблюдения предлагаемых мер.

Программно-технические методы включают предотвращение утечки информации путем исключения несанкционированного доступа к ней, предотвращение специальных воздействий, выявление внедренных программных или аппаратных закладных устройств для перехвата, съема или уничтожения информации, а также применение криптографических и иных средств защиты информации.

IV. ОСНОВЫ СОГЛАСОВАННОЙ ПОЛИТИКИ В ОБЛАСТИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВ-УЧАСТНИКОВ СОДРУЖЕСТВА НЕЗАВИСИМЫХ ГОСУДАРСТВ В ВОЕННОЙ СФЕРЕ

4.1. Основные положения согласованной политики в области обеспечения информационной безопасности государств-участников Содружества Независимых Государств в военной сфере.

Единство политики в области обеспечения информационной безопасности основывается на соблюдении интересов безопасности каждого государства-участника Содружества и исходит из принципа безусловного правового равенства всех участников информационного процесса вне зависимости от их политического, социального и экономического статуса. Политика формируется на основе ограничения доступа к информации, переданной им в рамках выполнения оборонных задач, и ответственности за защиту доверенных межгосударственных секретов.

Государства-участники Содружества по возможности стремятся к отказу от использования зарубежных информационных технологий для информатизации органов военного управления.

4.2. Правовое обеспечение информационной безопасности государств-участников Содружества Независимых Государств в военной сфере.

Правовую основу Концепции составляют соглашения и обязательства, а также международные договоры, заключенные или признанные государствами-участниками Содружества, определяющие права и ответственность граждан и государства в информационной сфере.

Правовое обеспечение информационной безопасности государств-участников Содружества в военной сфере базируется на соблюдении взаимных интересов.

Деятельность по правовому обеспечению информационной безопасности должна строиться на основе принципов законности и баланса интересов каждого государства-участника Содружества.

4.3. Первоочередные мероприятия по реализации Концепции.

Первоочередные мероприятия обеспечения информационной безопасности государств-участников Содружества в военной сфере предусматривают:

разработку и внедрение механизмов реализации и согласования правовых норм, регулирующих межгосударственные отношения в информационной сфере;

развитие правового обеспечения информационной безопасности на основе баланса интересов государств-участников Содружества;

создание Межгосударственного Консультативного совета по информационной безопасности государств-участников Содружества в военной сфере;

согласованное развитие инфраструктуры единого информационного пространства государств-участников Содружества;

совместное создание и внедрение безопасных технологий для информационных систем, используемых в военной сфере в интересах коллективной обороны.

V. ИСПОЛЬЗУЕМЫЕ ТЕРМИНЫ

Защита информации - деятельность по предотвращению утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Защита информации от несанкционированного доступа (НСД) - деятельность по предотвращению получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником (владельцем) информации прав или правил доступа к защищаемой информации.

Информация - сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информатизация - организационный, социально-экономический и научно-технический процесс создания оптимальных условий для удовлетворения информационных потребностей и реализации прав граждан, органов государственной власти, органов местного самоуправления, организаций, общественных объединений на основе формирования и использования информационных ресурсов.

Информационная безопасность - состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

Информационная инфраструктура - совокупность центров обработки и анализа информации, каналов информационного обмена и телекоммуникации, линий связи, систем и средств защиты информации.

Информационный потенциал - информация, зафиксированная на материальных носителях или в любой другой форме, обеспечивающей ее передачу во времени и пространстве потребителям для решения широкого спектра задач, связанных с деятельностью государственных институтов, военно-промышленного комплекса и вооруженных сил, силы и средства, используемые для добывания, передачи, обработки, хранения и отображения информации, а также умонастроения людей, использующих эту информацию и средства и способных запускать и контролировать вещественно-энергетические процессы.

Информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации.

Информационные ресурсы - отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информационная сфера (среда) - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

Информационная система - организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Информационная технология - организованная совокупность процессов, элементов, устройств и методов, используемых для обработки информации.

Конфиденциальная информация - документированная информация, правовой режим которой установлен специальными нормами действующего законодательства в области государственной, коммерческой, промышленной и другой деятельности.

Система защиты информации - совокупность органов и/или исполнителей, используемая ими техника защиты информации, а также объекты защиты, организованные и функционирующие по правилам, установленным соответствующими правовыми, организационно-распорядительными и нормативными документами о защите информации.

Система обеспечения информационной безопасности - совокупность правовых, организационных и технических мероприятий, органов, сил, средств и норм, направленных на предотвращение или существенное затруднение нанесения ущерба собственнику информации.