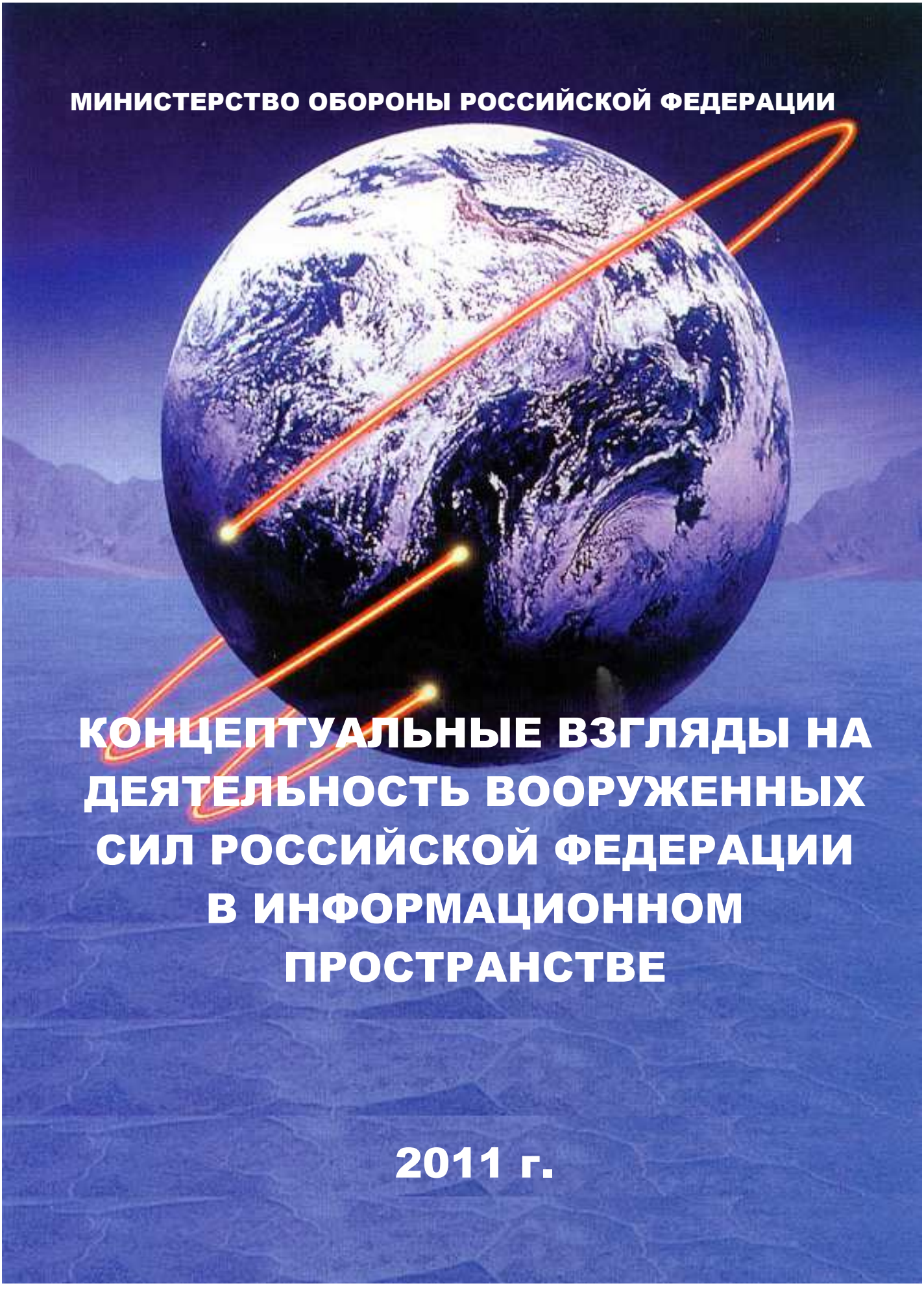
МИНИСТЕРСТВО ОБОРОНЫ РОССИЙСКОЙ ФЕДЕРАЦИИ



КОНЦЕПТУАЛЬНЫЕ ВЗГЛЯДЫ НА ДЕЯТЕЛЬНОСТЬ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ В ИНФОРМАЦИОННОМ ПРОСТРАНСТВЕ

2011 г.

СОДЕРЖАНИЕ

> *"Источником внешней угрозы информационной безопасности Российской Федерации является разработка рядом государств концепций информационных войн, предусматривающих создание средств опасного воздействия на информационные сферы других стран мира, нарушение нормального функционирования информационных и телекоммуникационных систем, сохранности информационных ресурсов, получение несанкционированного доступа к ним"*
>
> *(Доктрина информационной безопасности Российской Федерации, утвержденная Президентом Российской Федерации 9 сентября 2000 г.).*

Введение

Высокие темпы развития информационных систем различного назначения, компьютерных сетей типа Интернет и электронных СМИ привели на рубеже тысячелетий к формированию глобального информационного пространства. Наряду с сухопутным, морским, воздушным и космическим пространством, информационное пространство в армиях наиболее развитых стран стало активно использоваться для решения широкого круга военных задач.

Вследствие уязвимости информационно-коммуникационных систем к радиоэлектронным и программно-аппаратным воздействиям в мире возникло и стало быстро распространяться информационное оружие, обладающее трансграничными поражающими факторами, резко возросла роль информационной войны. Российская Федерация, стремительно продвигающаяся по пути информатизации всех сфер жизнедеятельности общества, оказалась перед лицом новой серьезной угрозы, исходящей из глобального информационного пространства.

Чрезвычайная важность противодействия актам агрессивной информационной войны впервые была отмечена в Доктрине информационной безопасности Российской Федерации, утвержденной Президентом Российской

Федерации 9 сентября 2000 г. В ней определено, что одним из приоритетных направлений противодействия данной угрозе является решение задач “совершенствования приемов и способов стратегической и оперативной маскировки, разведки и радиоэлектронной борьбы, методов и средств активного противодействия информационно-пропагандистским и психологическим операциям вероятного противника. Кроме того, в последнее время вследствие широкого применения в системах управления войсками и оружием компьютерной техники, этот перечень дополнился задачей защиты информационной инфраструктуры Вооруженных Сил Российской Федерации от различного рода компьютерных атак.

Опыт вооруженных конфликтов последнего десятилетия, а также практика оперативной подготовки войск и штабов позволяют констатировать, что в настоящее время в Вооруженных Силах Российской Федерации сложилась цельная система деятельности, призванная обеспечить эффективное сдерживание, предотвращение и разрешение военных конфликтов в информационном пространстве.

Настоящие Концептуальные взгляды раскрывают основные принципы, правила и меры доверия, в соответствии с которыми Вооруженные Силы Российской Федерации используют глобальное информационное пространство для решения задач обороны и безопасности.

1. Основные термины и определения

Для целей настоящего документа используются следующие основные термины и определения:

Военный конфликт в информационном пространстве - форма разрешения межгосударственных или внутригосударственных противоречий с применением информационного оружия.

Деятельность вооруженных сил в информационном пространстве – использование вооруженными силами информационных ресурсов для решения задач обороны и безопасности.

Информационная безопасность вооруженных сил - состояние защищенности информационных ресурсов вооруженных сил от воздействия информационного оружия.

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.

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.

Кризисная ситуация – этап эскалации конфликта, характеризующийся применением военной силы для его разрешения.

Международная информационная безопасность - состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Система обеспечения информационной безопасности Российской Федерации – часть системы обеспечения национальной безопасности

страны, предназначенная для реализации государственной политики в сфере информационной безопасности.

2 Принципы

Деятельность Вооруженных Сил Российской Федерации в информационном пространстве строится исходя из совокупности принципов: законности, приоритетности, комплексности, взаимодействия, сотрудничества, инновационности.

2.1 Законность

Соблюдение принципа законности требует от Вооруженных Сил Российской Федерации в ходе своих действий в информационном пространстве неукоснительно руководствоваться нормами и принципами действующего российского законодательства, а также общепризнанными нормами и принципами международного права.

В частности, в соответствии со ст.20 Военной доктрины Российской Федерации применение Вооруженных Сил Российской Федерации в мирное время осуществляется по решению Президента Российской Федерации в порядке, установленном федеральным законодательством. Так, решение на применение Вооруженных Сил Российской Федерации за пределами территории Российской Федерации принимается Президентом Российской Федерации на основании соответствующего постановления Совета Федерации Федерального Собрания Российской Федерации. Данное положение следует распространить также и на применение Вооруженных Сил Российской Федерации в информационном пространстве.

Что касается международного права, то Вооруженные Силы Российской Федерации применительно к особенностям военной деятельности в глобальном информационном пространстве руководствуются следующими его нормами и принципами:

уважение государственного суверенитета,

невмешательство во внутренние дела других государств,

неприменение силы и угрозы силой,

право на индивидуальную и коллективную самооборону.

Кроме того, Вооруженные Силы Российской Федерации руководствуются нормами международного гуманитарного права (ограничение неизбирательного применения информационного оружия; установление особой защиты для информационных объектов, являющихся потенциально опасными источниками техногенных катастроф; запрещение вероломных методов ведения информационной войны).

2.2 Приоритетность

Соблюдение принципа приоритетности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информационном пространстве в первоочередном порядке стремиться к сбору актуальной и достоверной информации об угрозах, ее оперативной обработке, глубокому анализу и своевременной выработке мер защиты. Все это в совокупности создает благоприятные условия для эффективного управления войсками и оружием, поддержания необходимого морально-психологического состояния личного состава.

Принятие комплекса мер по защите информационных ресурсов, позволит в условиях информационной войны избежать дезориентации органов военного управления, дезорганизации системы управления войсками и оружием, катастрофического разрушения элементов тыловой и транспортной инфраструктуры, деморализации личного состава и населения в зоне военных действий. В современных условиях необходимость принятия данных мер в приоритетном порядке обуславливается, в том числе тем, что сейчас сотни миллионов человек (целые страны и континенты) вовлечены в единое глобальное информационное пространство, образованное Интернетом, электронными СМИ и системами мобильной связи.

2.3 Комплексность

Соблюдение принципа комплексности требует от Вооруженных Сил Российской Федерации в ходе своей деятельности в информационном

пространстве использовать все имеющиеся силы и средства для эффективного решения стоящих перед ними задач.

В целом деятельность в информационном пространстве включает мероприятия штабов и действия войск по разведке, оперативной маскировке, радиоэлектронной борьбе, связи, скрытому и автоматизированному управлению, информационной работе штабов, а также защите своих информационных систем от радиоэлектронных, компьютерных и иных воздействий.

Деятельность в информационном пространстве представляет собой согласованную единую систему, в которой каждый компонент выполняет свои задачи присущими ему способами и приемами, а с другой стороны, интегрируясь в единую систему, повышает возможности всей системы по достижению целей, стоящих перед Вооруженными Силами Российской Федерации.

В организации деятельности в информационном пространстве в мирное, в военное время, при подготовке и в ходе операций (боевых действий) принимают непосредственное участие командование и штабы всех уровней.

Каждый из этих органов управления в соответствии со своими функциями и ответственностью разрабатывает и планирует мероприятия и действия подчиненных войск, объединенные единым замыслом действий в информационном пространстве.

2.4 Взаимодействие

Соблюдение принципа взаимодействия требует от Минобороны России согласовывать свои действия в информационном пространстве с другими федеральными органами исполнительной власти.

Взаимодействие осуществляется в рамках системы обеспечения информационной безопасности Российской Федерации, определенной Доктриной информационной безопасности Российской Федерации (2000 г.).

2.5 Сотрудничество

Соблюдение принципа сотрудничества требует согласования усилий с дружественными государствами и международными организациями.

Основной целью развития сотрудничества на глобальном уровне является установление международно-правового режима, регулирующего, в том числе, военную деятельность государств в мировом информационном пространстве на основе принципов и норм международного права.

Развитие сотрудничества на региональном уровне преследует следующие цели: создание механизмов принятия эффективных коллективных действий, направленных на выявление, предупреждение и пресечение применения информационно-телекоммуникационных технологий для угрозы миру и безопасности, осуществления актов агрессии урегулирование и разрешение международных споров и конфликтных ситуаций, связанных с враждебным использованием информационно-телекоммуникационных технологий, укрепление доверия в области использования информационных систем трансграничного характера и обеспечение безопасности использования единого информационного пространства.

2.6 Инновационность

Соблюдение принципа инновационности требует от Вооруженных Сил Российской Федерации использовать для подготовки и осуществления деятельности в информационном пространстве наиболее передовые технологии, средства и методики, а также привлекать к решению задач по информационной безопасности высококвалифицированный личный состав.

Поэтому для разработки и производства таких средств и технологий может привлекаться научно-производственный потенциал наиболее передовых инновационных центров Российской Федерации, а сама разработка осуществляться в рамках государственных и ведомственных программ и НИОКР.

Подготовка специалистов в сфере организации и осуществления деятельности в информационном пространстве проводится в образовательных учреждениях высшего профессионального образования Министерства обороны Российской Федерации.

Кроме того, для решения задач информационной безопасности Вооруженных Сил Российской Федерации могут привлекаться, в установленном законодательством Российской Федерации порядке, специалисты, закончившие иные образовательные учреждения Российской Федерации.

3 Правила

В ходе своей деятельности Вооруженные Силы Российской Федерации руководствуются совокупностью правил сдерживания, предотвращения и разрешения военных конфликтов в информационном пространстве

> *"Военная политика Российской Федерация направлена на недопущение гонки вооружений, сдерживание и предотвращение военных конфликтов …" (Военная доктрина Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 февраля 2010 г., ст.17)*

3.1 Сдерживание и предотвращение конфликтов

Вооруженные Силы Российской Федерации в своей практической деятельности руководствуются следующими правилами сдерживания и предотвращения военных конфликтов в информационном пространстве:

1. Развивать систему обеспечения информационной безопасности Вооруженных Сил Российской Федерации, предназначенную для сдерживания и разрешения военных конфликтов в информационном пространстве.

2. Поддерживать силы и средства обеспечения информационной безопасности в постоянной готовности к отражению угроз военно-политического характера в информационном пространстве.

3. Налаживать сотрудничество на приоритетной основе со странами Организации Договора о коллективной безопасности, Содружества Независимых Государств и Шанхайской организации сотрудничества, расширять круг государств-партнеров и развивать сотрудничество с ними на основе общих интересов в сфере укрепления международной информационной безопасности в соответствии с положениями Устава ООН и другими нормами международного права.

4. Стремиться к заключению под эгидой ООН договора об обеспечении международной информационной безопасности, распространяющего действие общепризнанных норм и принципов международного права на информационное пространство.

5. Принимать все возможные меры по раннему выявлению потенциальных военных конфликтов в информационном пространстве, а также разоблачению организаторов конфликта, подстрекателей и пособников.

6. Определять факторы возникновения и эскалации конфликта и устанавливать контроль над ними с тем, чтобы избежать возникновения чрезвычайных ситуаций.

7. Принимать первоочередные меры по противодействию развитию (консервации или обострению) конфликта и его переходу в такое состояние, которое значительно увеличивает цену урегулирования.

8. Принимать меры недопущения распространения конфликта на смежные сферы межгосударственных отношений, на урегулирование последствий которого потребуются дополнительные затраты и усилия.

9. Принимать меры по нейтрализации факторов, породивших конфликт, с тем, чтобы направить взаимодействие конфликтующих сторон в русло конструктивного сотрудничества.

10. Публично, объективно и своевременно разъяснять мировой общественности причины и истоки конфликта. Формирование необходимого общественного мнения подразумевает соответствующую его ориентацию и мобилизацию, позволяет создать в глобальном информационном пространстве климат, способствующий ограничению возможности совершения организаторами конфликта дальнейших эскалационных шагов.

3.2 Разрешение конфликтов

> *"Российская Федерация считает правомерным применение Вооруженных Сил и других войск для отражения агрессии против нее и (или) ее союзников, поддержания (восстановления) мира по решению Совета Безопасности ООН, других структур коллективной безопасности, а также для обеспечения защиты своих граждан, находящихся за пределами Российской Федерации, в соответствии с общепризнанными принципами и нормами международного права и международными договорами Российской Федерации"*
>
> *(Военная доктрина Российской Федерации, утвержденная Указом Президента Российской Федерации от 5 февраля 2010 г., ст. 20)*

Вооруженные Силы Российской Федерации руководствуются следующими правилами разрешения военных конфликтов в информационном пространстве:

1. Разрешение конфликтов в информационном пространстве осуществлять, в первую очередь, путем переговоров, примирения, обращения к Совету Безопасности ООН или к региональным органам, или соглашениям, или иными мирными средствами.

2. В случае усиления напряженности стремиться к недопущению перехода конфликта в крайние, разрушительные формы противоборства, и особенно те, которые могут привести к дестабилизации международной обстановки и возникновению кризисной ситуации.

3. В условиях эскалации конфликта в информационном пространстве и перехода его в кризисную фазу воспользоваться правом на индивидуальную или коллективную самооборону с применением любых избранных способов и средств, не противоречащих общепризнанным нормам и принципам международного права.

4. В интересах решения задач индивидуальной и коллективной самообороны определять необходимый потенциал ответных действий на основе национальных демократических процедур с учетом законных интересов обеспечения безопасности других государств, а также необходимости обеспечения международной информационной безопасности и стабильности.

5. В интересах индивидуальной и коллективной самообороны размещать свои силы и средства обеспечения информационной безопасности на территории других государств в соответствии с соглашениями, выработанными ими на добровольной основе в ходе переговоров, а также в соответствии с международным правом.

6. В ходе конфликта постоянно информировать отечественные и зарубежные СМИ о складывающейся ситуации и, опираясь на общественное мнение, эффективнее влиять на ее деэскалационное развитие и закрепление достигнутых результатов разрешения конфликтных противоречий.

4 Меры доверия

Вооруженные Силы Российской Федерации будут стремиться к выработке мер укрепления доверия в области военного использования информационного пространства. В частности, к таким мерам 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 сторон, и сотрудничество в отношении урегулирования конфликтных ситуаций военного характера.

Заключение

В современных условиях обороноспособность Российской Федерации существенно зависит от эффективности деятельности Вооруженных Сил в информационном пространстве и во многом определяется их возможностями по сдерживанию, предотвращению и разрешению конфликтов, возникающих в информационном пространстве.

Вооруженные Силы Российской Федерации планируют решать стоящие перед ними задачи обеспечения обороны и безопасности, опираясь на основополагающие принципы и правила деятельности Вооруженных Сил Российской Федерации в информационном пространстве, а также меры доверия, изложенные в настоящих Концептуальных взглядах.

Реализуя настоящие Концептуальные взгляды, Вооруженные Силы Российской Федерации будет стремиться к максимальному использованию возможностей информационного пространства для укрепления обороноспособности государства, сдерживания и предотвращения военных конфликтов, развития военного сотрудничества, а также формирования системы международной информационной безопасности в интересах всего мирового сообщества.