



ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

 **Del-89**
МОСКВА

Доктрина информационной безопасности Российской Федерации

является базовым концептуальным документом, который определяет основные направления обеспечения одного из ключевых направлений безопасности российского государства.

Она была одобрена Советом Безопасности РФ **23 июня** и утверждена президентом России В. Путиным **9 сентября 2000 г.**

Доктрина информационной безопасности Российской Федерации

Доктрина информационной безопасности Российской Федерации представляет собой совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина **служит** основой для:

- формирования государственной политики в области обеспечения информационной безопасности Российской Федерации;
- подготовки предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации;
- разработки целевых программ обеспечения информационной безопасности Российской Федерации.

Настоящая Доктрина **развивает**
Концепцию национальной безопасности
Российской Федерации применительно
к информационной сфере.

СТРУКТУРА ДОКТРИНЫ

- I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ**
 1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение
 2. Виды угроз информационной безопасности Российской Федерации
 3. Источники угроз информационной безопасности Российской Федерации
 4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

II. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

- 5. Общие методы обеспечения информационной безопасности Российской Федерации**
- 6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни**
- 7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности**

III. ОСНОВНЫЕ ПОЛОЖЕНИЯ ГОСУДАРСТВЕННОЙ ПОЛИТИКИ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ И ПЕРВООЧЕРЕДНЫЕ МЕРОПРИЯТИЯ ПО ЕЕ РЕАЛИЗАЦИИ

**8. Основные положения государственной политики
обеспечения информационной безопасности
Российской Федерации**

**9. Первоочередные мероприятия по реализации
государственной политики обеспечения
информационной безопасности Российской Федерации**

IV. ОРГАНИЗАЦИОННАЯ ОСНОВА СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

**10. Основные функции системы обеспечения
информационной безопасности Российской
Федерации**

**11. Основные элементы организационной основы
системы обеспечения информационной
безопасности Российской Федерации**

I. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Под информационной безопасностью Российской Федерации понимается состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства.

1. Национальные интересы Российской Федерации в информационной сфере и их обеспечение

Выделяются четыре основные составляющие национальных интересов Российской Федерации в информационной сфере.

Первая составляющая в информационной сфере включает в себя соблюдение конституционных прав и свобод человека и гражданина в области получения информации и пользования ею, обеспечение духовного обновления России, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Вторая составляющая в информационной сфере включает в себя **информационное обеспечение государственной политики Российской Федерации**, связанное с доведением до российской и международной общественности достоверной информации о государственной политике Российской Федерации, ее официальной позиции по социально значимым событиям российской и международной жизни, с обеспечением доступа граждан к открытым государственным информационным ресурсам.

Третья составляющая в информационной сфере включает в себя **развитие современных информационных технологий**, отечественной индустрии информации, в том числе индустрии средств информатизации, телекоммуникации и связи, обеспечение потребностей внутреннего рынка ее продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранности и эффективного использования отечественных информационных ресурсов.

Четвертая составляющая в информационной сфере включает в себя **защиту информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создаваемых на территории России.**

2. Виды угроз информационной безопасности Российской Федерации

По своей общей направленности угрозы информационной безопасности Российской Федерации подразделяются на следующие виды:

угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению России;

угрозы информационному обеспечению государственной политики Российской Федерации;

угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России.

Понятие субъектов информационных отношений

- Под термином «**субъект**» понимаются государство (в целом или отдельные его органы и организации), общественные или коммерческие организации (объединения) и предприятия (юридические лица), отдельные граждане (физические лица).
- В процессе своей деятельности субъекты могут находиться друг с другом в разного рода отношениях, в том числе, касающихся вопросов **получения, хранения, обработки, распространения и использования определенной информации**.
- Такие отношения между субъектами называются **информационными отношениями**, а сами участвующие в них субъекты - **субъектами информационных отношений**.

3. Источники угроз информационной безопасности Российской Федерации

Источники угроз информационной безопасности Российской Федерации подразделяются на:

- **внешние;**
- **внутренние.**

К внешним источникам относятся:

- деятельность иностранных политических, экономических, военных, разведывательных и информационных структур, направленная против интересов Российской Федерации в информационной сфере;
 - стремление ряда стран к доминированию и ущемлению интересов России в мировом информационном пространстве, вытеснению ее с внешнего и внутреннего информационных рынков;
 - обострение международной конкуренции за обладание информационными технологиями и ресурсами;
 - деятельность международных террористических организаций;

- - увеличение технологического отрыва ведущих держав мира и наращивание их возможностей по противодействию созданию конкурентоспособных российских информационных технологий;
 - деятельность космических, воздушных, морских и наземных технических и иных средств (видов) разведки иностранных государств;
 - 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.

К внутренним источникам относятся:

- критическое состояние отечественных отраслей промышленности;

- неблагоприятная криминогенная обстановка, сопровождаемая тенденциями сращивания государственных и криминальных структур в информационной сфере, получения криминальными структурами доступа к конфиденциальной информации, усиления влияния организованной преступности на жизнь общества, снижения степени защищенности законных интересов граждан, общества и государства в информационной сфере;

- недостаточная координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации по формированию и реализации единой государственной политики в области обеспечения информационной безопасности Российской Федерации;

- недостаточная разработанность нормативной правовой базы, регулирующей отношения в информационной сфере, а также недостаточная правоприменительная практика;

- неразвитость институтов гражданского общества и недостаточный государственный контроль за развитием информационного рынка России;

- недостаточное финансирование мероприятий по обеспечению информационной безопасности Российской Федерации;
недостаточная экономическая мощь государства;
- снижение эффективности системы образования и воспитания, недостаточное количество квалифицированных кадров в области обеспечения информационной безопасности;
- недостаточная активность федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации в информировании общества о своей деятельности, в разъяснении принимаемых решений, в формировании открытых государственных ресурсов и развитии системы доступа к ним граждан;
- отставание России от ведущих стран мира по уровню информатизации федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации и органов местного самоуправления, кредитно-финансовой сферы, промышленности, сельского хозяйства, образования, здравоохранения, сферы услуг и быта граждан.

4. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению

- Приняты Закон Российской Федерации "О государственной тайне", Основы законодательства Российской Федерации об Архивном фонде Российской Федерации и архивах, федеральные законы "Об информации, информатизации и защите информации", "Об участии в международном информационном обмене", ряд других законов, развернута работа по созданию механизмов их реализации, подготовке законопроектов, регламентирующих общественные отношения в информационной сфере.
- Осуществлены мероприятия по обеспечению информационной безопасности в федеральных органах государственной власти, органах государственной власти субъектов Российской Федерации, на предприятиях, в учреждениях и организациях независимо от формы собственности.
- Развернуты работы по созданию защищенной информационно-телекоммуникационной системы специального назначения в интересах органов государственной власти.

Вместе с тем анализ состояния информационной безопасности Российской Федерации показывает, что ее уровень **не в полной мере соответствует потребностям общества и государства.**

Современные условия политического и социально-экономического развития страны вызывают **обострение противоречий** между потребностями общества в расширении свободного обмена информацией и необходимостью сохранения отдельных регламентированных ограничений на ее распространение.

Противоречивость и неразвитость правового регулирования общественных отношений в информационной сфере приводят к серьезным негативным последствиям.

Необеспеченность прав граждан на доступ к информации, манипулирование информацией вызывают негативную реакцию населения, что в ряде случаев ведет к дестабилизации социально-политической обстановки в обществе.

- Закрепленные в Конституции Российской Федерации права граждан на неприкосновенность частной жизни, личную и семейную тайну, тайну переписки практически не имеют достаточного правового, организационного и технического обеспечения.
- Неудовлетворительно организована защита собираемых федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, органами местного самоуправления данных о физических лицах (персональных данных).
- Нет четкости при проведении государственной политики в области формирования российского информационного пространства, развития системы массовой информации, организации международного информационного обмена и интеграции информационного пространства России в мировое информационное пространство, что создает условия для вытеснения российских информационных агентств, средств массовой информации с внутреннего информационного рынка и деформации структуры международного информационного обмена.

- Недостаточна государственная поддержка деятельности российских информационных агентств по продвижению их продукции на зарубежный информационный рынок.
- Ухудшается ситуация с обеспечением сохранности сведений, составляющих государственную тайну.
- Серьезный урон нанесен кадровому потенциалу научных и производственных коллективов, действующих в области создания средств информатизации, телекоммуникации и связи, в результате массового ухода из этих коллективов наиболее квалифицированных специалистов.

- Отставание отечественных информационных технологий вынуждает федеральные органы государственной власти, органы государственной власти субъектов Российской Федерации и органы местного самоуправления при создании информационных систем идти по пути закупок импортной техники и привлечения иностранных фирм, из-за чего повышается вероятность несанкционированного доступа к обрабатываемой информации и возрастает зависимость России от иностранных производителей компьютерной и телекоммуникационной техники, а также программного обеспечения.

- В связи с интенсивным внедрением зарубежных информационных технологий в сферы деятельности личности, общества и государства, а также с широким применением открытых информационно-телекоммуникационных систем, интеграцией отечественных информационных систем и международных информационных систем возросли угрозы применения "информационного оружия" против информационной инфраструктуры России. Работы по адекватному комплексному противодействию этим угрозам ведутся при недостаточной координации и слабом бюджетном финансировании. Недостаточное внимание уделяется развитию средств космической разведки и радиоэлектронной борьбы.

Сложившееся положение дел в области обеспечения информационной безопасности Российской Федерации требует безотлагательного решения таких задач, как:

- разработка основных направлений государственной политики в области обеспечения информационной безопасности Российской Федерации, а также мероприятий и механизмов, связанных с реализацией этой политики;
- развитие и совершенствование системы обеспечения информационной безопасности Российской Федерации, реализующей единую государственную политику в этой области, включая совершенствование форм, методов и средств выявления, оценки и прогнозирования угроз информационной безопасности Российской Федерации, а также системы противодействия этим угрозам;
- разработка федеральных целевых программ обеспечения информационной безопасности Российской Федерации;
- разработка критериев и методов оценки эффективности систем и средств обеспечения информационной безопасности Российской Федерации, а также сертификации этих систем и средств;

- совершенствование нормативной правовой базы обеспечения информационной безопасности Российской Федерации, включая механизмы реализации прав граждан на получение информации и доступ к ней, формы и способы реализации правовых норм, касающихся взаимодействия государства со средствами массовой информации;
- установление ответственности должностных лиц федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, юридических лиц и граждан за соблюдение требований информационной безопасности;
- координация деятельности федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, предприятий, учреждений и организаций независимо от формы собственности в области обеспечения информационной безопасности Российской Федерации;

- развитие научно-практических основ обеспечения информационной безопасности Российской Федерации с учетом современной геополитической ситуации, условий политического и социально-экономического развития России и реальности угроз применения "информационного оружия";

разработка методов повышения эффективности участия государства в формировании информационной политики государственных телерадиовещательных организаций, других государственных средств массовой информации;

обеспечение технологической независимости Российской Федерации в важнейших областях информатизации, телекоммуникации и связи, определяющих ее безопасность, и в первую очередь в области создания специализированной вычислительной техники для образцов вооружения и военной техники;

разработка современных методов и средств защиты информации, обеспечения безопасности информационных технологий, и прежде всего используемых в системах управления войсками и оружием, экологически опасными и экономически важными производствами;

развитие и совершенствование государственной системы защиты информации и системы защиты государственной тайны;

создание и развитие современной защищенной технологической основы управления государством в мирное время, в чрезвычайных ситуациях и в военное время;

- расширение взаимодействия с международными и зарубежными органами и организациями при решении научно-технических и правовых вопросов обеспечения безопасности информации, передаваемой с помощью международных телекоммуникационных систем и систем связи;
- обеспечение условий для активного развития российской информационной инфраструктуры, участия России в процессах создания и использования глобальных информационных сетей и систем;
- создание единой системы подготовки кадров в области информационной безопасности и информационных технологий.

II. МЕТОДЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ

5. Общие методы обеспечения информационной безопасности Российской Федерации

Общие методы обеспечения информационной безопасности Российской Федерации разделяются на:

- правовые,
- организационно-технические,
- экономические.

К правовым методам обеспечения
информационной безопасности Российской
Федерации относится разработка нормативных
правовых актов, регламентирующих отношения в
информационной сфере, и нормативных
методических документов по вопросам обеспечения
информационной безопасности Российской
Федерации

Организационно-техническими методами обеспечения информационной безопасности Российской Федерации являются:

- создание и совершенствование системы обеспечения информационной безопасности Российской Федерации;**
- усиление правоприменительной деятельности федеральных органов исполнительной власти, органов исполнительной власти субъектов Российской Федерации, включая предупреждение и пресечение правонарушений в информационной сфере, а также выявление, изобличение и привлечение к ответственности лиц, совершивших преступления и другие правонарушения в этой сфере;**
- разработка, использование и совершенствование средств защиты информации и методов контроля эффективности этих средств, развитие защищенных телекоммуникационных систем, повышение надежности специального программного обеспечения;**
- создание систем и средств предотвращения несанкционированного доступа к обрабатываемой информации и специальных воздействий, вызывающих разрушение, уничтожение, искажение информации, а также изменение штатных режимов функционирования систем и средств информатизации и связи;**

- выявление технических устройств и программ, представляющих опасность для нормального функционирования информационно-телекоммуникационных систем, предотвращение перехвата информации по техническим каналам, применение криптографических средств защиты информации при ее хранении, обработке и передаче по каналам связи, контроль за выполнением специальных требований по защите информации;
- сертификация средств защиты информации, лицензирование деятельности в области защиты государственной тайны, стандартизация способов и средств защиты информации;

- **совершенствование системы сертификации телекоммуникационного оборудования и программного обеспечения автоматизированных систем обработки информации по требованиям информационной безопасности;**
 - **контроль за действиями персонала в защищенных информационных системах, подготовка кадров в области обеспечения информационной безопасности Российской Федерации;**
 - **формирование системы мониторинга показателей и характеристик информационной безопасности Российской Федерации в наиболее важных сферах жизни и деятельности общества и государства.**

Экономические методы обеспечения информационной безопасности Российской Федерации включают в себя:

- разработку программ обеспечения информационной безопасности Российской Федерации и определение порядка их финансирования;**
- совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования информационных рисков физических и юридических лиц.**

6. Особенности обеспечения информационной безопасности Российской Федерации в различных сферах общественной жизни

- В сфере экономики.**
- В сфере внутренней политики.**
- В сфере внешней политики.**
- В области науки и техники.**
- В сфере духовной жизни.**
- В сфере обороны.**
- В правоохранительной и судебной сферах.**
- В условиях чрезвычайных ситуаций.**

7. Международное сотрудничество Российской Федерации в области обеспечения информационной безопасности

Основными направлениями международного сотрудничества Российской Федерации в области обеспечения информационной безопасности являются:

запрещение разработки, распространения и применения "информационного оружия";

обеспечение безопасности международного информационного обмена, в том числе сохранности информации при ее передаче по национальным телекоммуникационным каналам и каналам связи;

координация деятельности правоохранительных органов стран, входящих в мировое сообщество, по предотвращению компьютерных преступлений;

- предотвращение несанкционированного доступа к конфиденциальной информации в международных банковских телекоммуникационных сетях и системах информационного обеспечения мировой торговли, к информации международных правоохранительных организаций, ведущих борьбу с транснациональной организованной преступностью, международным терроризмом, распространением наркотиков и психотропных веществ, незаконной торговлей оружием и расщепляющимися материалами, а также торговлей людьми.



1 февраля президент России Дмитрий Медведев утвердил доктрину продовольственной безопасности. Задачи утвержденной Медведевым доктрины – обеспечить население страны бесперебойными поставками продуктов питания, развитие отечественного агропромышленного и рыбохозяйственного комплексов, иметь возможность оперативно реагировать на внутренние и внешние угрозы стабильности продовольственного рынка, говорится в указе президента.

Согласно указу, необходимо к 2020 году добиться, чтобы на полках магазинов было не менее 80% товаров российского производства, и только 20% оставалось импортного. Так, Россия должна быть обеспеченной зерном внутреннего производства не менее чем на 95%, российским сахаром – не менее чем на 80%, местным растительным маслом – на 80%, мясом и мясными продуктами, выпущенными в России – на 85% -, молоком внутреннего производства – на 90%, рыбной продукцией – на 80%, картофелем – на 95%, пищевой солью – на 85%, говорится в документе. Таким образом, импорт по основным продуктам питания должен существенно сократиться.