**Доктрина информационной безопасности Российской Федерации**

### *Общие положения*

Доктрина представляет собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

В Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации - объективно значимые потребности личности, общества и государства в обеспечении их защищенности и устойчивого развития в части, касающейся информационной сферы;

б) угроза информационной безопасности Российской Федерации - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства;

г) обеспечение информационной безопасности - осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаружению, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления;

д) силы обеспечения информационной безопасности - государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности;

е) средства обеспечения информационной безопасности - правовые, организационные, технические и другие средства, используемые силами обеспечения информационной безопасности;

ж) система обеспечения информационной безопасности - совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности;

з) информационная инфраструктура Российской Федерации - совокупность объектов информатизации, информационных систем, сайтов в сети «Интернет» и сетей связи, расположенных на территории Российской Федерации, а также на территориях, находящихся под юрисдикцией Российской Федерации или используемых на основании международных договоров Российской Федерации.

Правовую основу настоящей Доктрины составляют Конституция Российской Федерации, общепризнанные принципы и нормы международного права, международные договоры Российской Федерации, федеральные конституционные законы, федеральные законы, а также нормативные правовые акты Президента Российской Федерации и Правительства Российской Федерации.

1. ***Национальные интересы в информационной сфере***

Национальными интересами в информационной сфере являются:

а) обеспечение и защита конституционных прав и свобод человека и гражданина в части, касающейся получения и использования информации, неприкосновенности частной жизни при использовании информационных технологий, обеспечение информационной поддержки демократических институтов, механизмов взаимодействия государства и гражданского общества, а также применение информационных технологий в интересах сохранения культурных, исторических и духовно-нравственных ценностей многонационального народа Российской Федерации;

б) обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее - критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время;

в) развитие в Российской Федерации отрасли информационных технологий и электронной промышленности, а также совершенствование деятельности производственных, научных и научно-технических организаций по разработке, производству и эксплуатации средств обеспечения информационной безопасности, оказанию услуг в области обеспечения информационной безопасности;

г) доведение до российской и международной общественности достоверной информации о государственной политике Российской Федерации и ее официальной позиции по социально значимым событиям в стране и мире, применение информационных технологий в целях обеспечения национальной безопасности Российской Федерации в области культуры;

д) содействие формированию системы международной информационной безопасности, направленной на противодействие угрозам использования информационных технологий в целях нарушения стратегической стабильности, на укрепление равноправного стратегического партнерства в области информационной безопасности, а также на защиту суверенитета Российской Федерации в информационном пространстве.

### *3. Основные информационные угрозы и состояние информационной безопасности*

### Основными информационными угрозами являются:

1. Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

2. Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств.

3. Наращивание информационного воздействия на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

4. Возрастание масштабов компьютерной преступности в кредитно-финансовой сфере;

5. Увеличение числа преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина.

Состояние информационной безопасности в области обороны страны характеризуется увеличением масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях, в том числе для осуществления действий, противоречащих международному праву, направленных на подрыв суверенитета, политической и социальной стабильности, территориальной целостности Российской Федерации и ее союзников и представляющих угрозу международному миру, глобальной и региональной безопасности.

Состояние информационной безопасности в области государственной и общественной безопасности характеризуется постоянным повышением сложности, увеличением масштабов и ростом скоординированности компьютерных атак на объекты критической информационной инфраструктуры, усилением разведывательной деятельности иностранных государств в отношении Российской Федерации, а также нарастанием угроз применения информационных технологий в целях нанесения ущерба суверенитету, территориальной целостности, политической и социальной стабильности Российской Федерации.

Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг.

Состояние информационной безопасности в области науки, технологий и образования характеризуется недостаточной эффективностью научных исследований, направленных на создание перспективных информационных технологий, низким уровнем внедрения отечественных разработок и недостаточным кадровым обеспечением в области информационной безопасности, а также низкой осведомленностью граждан в вопросах обеспечения личной информационной безопасности.

Состояние информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства характеризуется стремлением отдельных государств использовать технологическое превосходство для доминирования в информационном пространстве.

### *Стратегические цели и основные направления обеспечения информационной безопасности*

Стратегической целью обеспечения информационной безопасности в области обороны страны является защита жизненно важных интересов личности, общества и государства от внутренних и внешних угроз, связанных с применением информационных технологий в военно-политических целях, противоречащих международному праву, в том числе в целях осуществления враждебных действий и актов агрессии, направленных на подрыв суверенитета, нарушение территориальной целостности государств и представляющих угрозу международному миру, безопасности и стратегической стабильности.

Стратегическими целями обеспечения информационной безопасности в области государственной и общественной безопасности являются защита суверенитета, поддержание политической и социальной стабильности, территориальной целостности Российской Федерации, обеспечение основных прав и свобод человека и гражданина, а также защита критической информационной инфраструктуры.

Стратегическими целями обеспечения информационной безопасности в экономической сфере являются сведение к минимально возможному уровню влияния негативных факторов, обусловленных недостаточным уровнем развития отечественной отрасли информационных технологий и электронной промышленности, разработка и производство конкурентоспособных средств обеспечения информационной безопасности, а также повышение объемов и качества оказания услуг в области обеспечения информационной безопасности.

Стратегической целью обеспечения информационной безопасности в области науки, технологий и образования является поддержка инновационного и ускоренного развития системы обеспечения информационной безопасности, отрасли информационных технологий и электронной промышленности.

Стратегической целью обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства является формирование устойчивой системы неконфликтных межгосударственных отношений в информационном пространстве.

### *Организационные основы обеспечения информационной безопасности*

Обеспечение информационной безопасности осуществляется на основе сочетания законодательной, правоприменительной, правоохранительной, судебной, контрольной и других форм деятельности государственных органов во взаимодействии с органами местного самоуправления, организациями и гражданами.

Система обеспечения информационной безопасности строится на основе разграничения полномочий органов законодательной, исполнительной и судебной власти в данной сфере с учетом предметов ведения федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, а также органов местного самоуправления, определяемых законодательством Российской Федерации в области обеспечения безопасности.

Организационную основу системы обеспечения информационной безопасности составляют: Совет Федерации Федерального Собрания Российской Федерации, Государственная Дума Федерального Собрания Российской Федерации, Правительство Российской Федерации, Совет Безопасности Российской Федерации, федеральные органы исполнительной власти, Центральный банк Российской Федерации, Военно-промышленная комиссия Российской Федерации, межведомственные органы, создаваемые Президентом Российской Федерации и Правительством Российской Федерации, органы исполнительной власти субъектов Российской Федерации, органы местного самоуправления, органы судебной власти, принимающие в соответствии с законодательством Российской Федерации участие в решении задач по обеспечению информационной безопасности.

Участниками системы обеспечения информационной безопасности являются: собственники объектов критической информационной инфраструктуры и организации, эксплуатирующие такие объекты, средства массовой информации и массовых коммуникаций, организации денежно-кредитной, валютной, банковской и иных сфер финансового рынка, операторы связи, операторы информационных систем, организации, осуществляющие деятельность по созданию и эксплуатации информационных систем и сетей связи, по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, организации, осуществляющие образовательную деятельность в данной области, общественные объединения, иные организации и граждане, которые в соответствии с законодательством Российской Федерации участвуют в решении задач по обеспечению информационной безопасности.