



**КонсультантПлюс**  
надежная правовая поддержка

Указ Президента РФ от 05.12.2016 N 646  
"Об утверждении Доктрины информационной  
безопасности Российской Федерации"

Документ предоставлен **КонсультантПлюс**

[www.consultant.ru](http://www.consultant.ru)

Дата сохранения: □ 26.07.2018

---

5 декабря 2016 года N 646

---

**УКАЗ**  
**ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ**  
**ОБ УТВЕРЖДЕНИИ ДОКТРИНЫ**  
**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

В целях обеспечения информационной безопасности Российской Федерации постановляю:

1. Утвердить прилагаемую **Доктрину** информационной безопасности Российской Федерации.
2. Признать утратившей силу **Доктрину** информационной безопасности Российской Федерации, утвержденную Президентом Российской Федерации 9 сентября 2000 г. N Пр-1895.
3. Настоящий Указ вступает в силу со дня его подписания.

Президент  
Российской Федерации  
В.ПУТИН

Москва, Кремль

5 декабря 2016 года

N 646

Утверждена  
Указом Президента  
Российской Федерации  
от 5 декабря 2016 г. N 646

**ДОКТРИНА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИЙСКОЙ ФЕДЕРАЦИИ**

I. Общие положения

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

В настоящей Доктрине под информационной сферой понимается совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети "Интернет" (далее - сеть "Интернет"), сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и

---

обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений.

2. В настоящей Доктрине используются следующие основные понятия:

а) национальные интересы Российской Федерации в информационной сфере (далее - национальные интересы в информационной сфере) - 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 (далее - информационная угроза) - совокупность действий и факторов, создающих опасность нанесения ущерба национальным интересам в информационной сфере;

в) информационная безопасность Российской Федерации (далее - информационная безопасность) - 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 взаимосвязанных правовых, организационных, оперативно-разыскных, 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 (далее - информационная инфраструктура) - 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.

3. В настоящей Доктрине на основе анализа основных информационных угроз и оценки состояния информационной безопасности определены стратегические цели и основные направления обеспечения информационной безопасности с учетом стратегических национальных приоритетов

---

Российской Федерации.

4. 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.

5. Настоящая Доктрина является документом стратегического планирования в сфере обеспечения национальной безопасности Российской Федерации, в котором развиваются положения **Стратегии** национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. N 683, а также других документов стратегического планирования в указанной сфере.

6. Настоящая Доктрина является основой для формирования государственной политики и развития общественных отношений в области обеспечения информационной безопасности, а также для выработки мер по совершенствованию системы обеспечения информационной безопасности.

## II. Национальные интересы в информационной сфере

7. Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества.

Информационная сфера играет важную роль в обеспечении реализации стратегических национальных приоритетов Российской Федерации.

8. 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.

9. Реализация национальных интересов в информационной сфере направлена на формирование безопасной среды оборота достоверной информации и устойчивой к различным видам воздействия информационной инфраструктуры в целях обеспечения конституционных прав и свобод человека и гражданина, стабильного социально-экономического развития страны, а также национальной безопасности Российской Федерации.

### III. Основные информационные угрозы и состояние информационной безопасности

10. Расширение областей применения информационных технологий, являясь фактором развития экономики и совершенствования функционирования общественных и государственных институтов, одновременно порождает новые информационные угрозы.

Возможности трансграничного оборота информации все чаще используются для достижения геополитических, противоречащих международному праву военно-политических, а также террористических, экстремистских, криминальных и иных противоправных целей в ущерб международной безопасности и стратегической стабильности.

При этом практика внедрения информационных технологий без увязки с обеспечением информационной безопасности существенно повышает вероятность проявления информационных угроз.

11. Одним из основных негативных факторов, влияющих на состояние информационной безопасности, является наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях.

Одновременно с этим усиливается деятельность организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий оборонно-промышленного комплекса.

12. Расширяются масштабы использования специальными службами отдельных государств средств оказания информационно-психологического воздействия, направленного на дестабилизацию внутривнутриполитической и социальной ситуации в различных регионах мира и приводящего к подрыву суверенитета и нарушению территориальной целостности других государств. В эту деятельность вовлекаются религиозные, этнические, правозащитные и иные организации, а также отдельные группы граждан, при этом широко используются возможности информационных технологий.

Отмечается тенденция к увеличению в зарубежных средствах массовой информации объема материалов, содержащих предвзятую оценку государственной политики Российской Федерации.

---

Российские средства массовой информации зачастую подвергаются за рубежом откровенной дискриминации, российским журналистам создаются препятствия для осуществления их профессиональной деятельности.

Нарастает информационное воздействие на население России, в первую очередь на молодежь, в целях размывания традиционных российских духовно-нравственных ценностей.

13. Различные террористические и экстремистские организации широко используют механизмы информационного воздействия на индивидуальное, групповое и общественное сознание в целях нагнетания межнациональной и социальной напряженности, разжигания этнической и религиозной ненависти либо вражды, пропаганды экстремистской идеологии, а также привлечения к террористической деятельности новых сторонников. Такими организациями в противоправных целях активно создаются средства деструктивного воздействия на объекты критической информационной инфраструктуры.

14. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека и гражданина, в том числе в части, касающейся неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий. При этом методы, способы и средства совершения таких преступлений становятся все изощреннее.

15. 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.

16. 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.

17. Состояние информационной безопасности в экономической сфере характеризуется недостаточным уровнем развития конкурентоспособных информационных технологий и их использования для производства продукции и оказания услуг. Остается высоким уровень зависимости отечественной промышленности от зарубежных информационных технологий в части, касающейся электронной компонентной базы, программного обеспечения, вычислительной техники и средств связи, что обуславливает зависимость социально-экономического развития Российской Федерации от геополитических интересов зарубежных стран.

18. 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. При этом мероприятия по обеспечению безопасности информационной инфраструктуры, включая ее целостность, доступность и устойчивое функционирование, с использованием отечественных информационных технологий и отечественной продукции зачастую не имеют комплексной основы.

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

Существующее в настоящее время распределение между странами ресурсов, необходимых для обеспечения безопасного и устойчивого функционирования сети "Интернет", не позволяет реализовать совместное справедливое, основанное на принципах доверия управление ими.

Отсутствие международно-правовых норм, регулирующих межгосударственные отношения в информационном пространстве, а также механизмов и процедур их применения, учитывающих специфику информационных технологий, затрудняет формирование системы международной информационной безопасности, направленной на достижение стратегической стабильности и равноправного стратегического партнерства.

#### IV. Стратегические цели и основные направления обеспечения информационной безопасности

20. 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.

21. В соответствии с военной политикой Российской Федерации основными направлениями обеспечения информационной безопасности в области обороны страны являются:

а) стратегическое сдерживание и предотвращение военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование системы обеспечения информационной безопасности Вооруженных Сил Российской Федерации, других войск, воинских формирований и органов, включающей в себя силы и средства информационного противоборства;

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере;

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере;

д) нейтрализация информационно-психологического воздействия, в том числе направленного на подрыв исторических основ и патриотических традиций, связанных с защитой Отечества.

КонсультантПлюс: примечание.

О безопасности критической информационной инфраструктуры Российской Федерации см. Федеральный закон от 26.07.2017 N 187-ФЗ.

22. 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.

23. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации;

б) пресечение деятельности, наносящей ущерб национальной безопасности Российской Федерации, осуществляемой с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами;

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры;

г) повышение безопасности функционирования объектов информационной инфраструктуры, в том числе в целях обеспечения устойчивого взаимодействия государственных органов, недопущения иностранного контроля за функционированием таких объектов, обеспечение целостности, устойчивости функционирования и безопасности единой сети электросвязи Российской Федерации, а также обеспечение безопасности информации, передаваемой по ней и обрабатываемой в информационных системах на территории Российской Федерации;

д) повышение безопасности функционирования образцов вооружения, военной и специальной техники и автоматизированных систем управления;

е) повышение эффективности профилактики правонарушений, совершаемых с использованием информационных технологий, и противодействия таким правонарушениям;

ж) обеспечение защиты информации, содержащей сведения, составляющие государственную тайну, иной информации ограниченного доступа и распространения, в том числе за счет повышения защищенности соответствующих информационных технологий;

з) совершенствование методов и способов производства и безопасного применения продукции, оказания услуг на основе информационных технологий с использованием отечественных разработок, удовлетворяющих требованиям информационной безопасности;



и) повышение эффективности информационного обеспечения реализации государственной политики Российской Федерации;

к) нейтрализация информационного воздействия, направленного на размывание традиционных российских духовно-нравственных ценностей.

24. 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.

25. Основными направлениями обеспечения информационной безопасности в экономической сфере являются:

а) инновационное развитие отрасли информационных технологий и электронной промышленности, увеличение доли продукции этой отрасли в валовом внутреннем продукте, в структуре экспорта страны;

б) ликвидация зависимости отечественной промышленности от зарубежных информационных технологий и средств обеспечения информационной безопасности за счет создания, развития и широкого внедрения отечественных разработок, а также производства продукции и оказания услуг на их основе;

в) повышение конкурентоспособности российских компаний, осуществляющих деятельность в отрасли информационных технологий и электронной промышленности, разработку, производство и эксплуатацию средств обеспечения информационной безопасности, оказывающих услуги в области обеспечения информационной безопасности, в том числе за счет создания благоприятных условий для осуществления деятельности на территории Российской Федерации;

г) развитие отечественной конкурентоспособной электронной компонентной базы и технологий производства электронных компонентов, обеспечение потребности внутреннего рынка в такой продукции и выхода этой продукции на мировой рынок.

26. 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.

27. Основными направлениями обеспечения информационной безопасности в области науки, технологий и образования являются:

а) достижение конкурентоспособности российских информационных технологий и развитие научно-технического потенциала в области обеспечения информационной безопасности;

б) создание и внедрение информационных технологий, изначально устойчивых к различным видам воздействия;

в) проведение научных исследований и осуществление опытных разработок в целях создания

---

перспективных информационных технологий и средств обеспечения информационной безопасности;

г) развитие кадрового потенциала в области обеспечения информационной безопасности и применения информационных технологий;

д) обеспечение защищенности граждан от информационных угроз, в том числе за счет формирования культуры личной информационной безопасности.

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

29. Основными направлениями обеспечения информационной безопасности в области стратегической стабильности и равноправного стратегического партнерства являются:

а) защита суверенитета Российской Федерации в информационном пространстве посредством осуществления самостоятельной и независимой политики, направленной на реализацию национальных интересов в информационной сфере;

б) участие в формировании системы международной информационной безопасности, обеспечивающей эффективное противодействие использованию информационных технологий в военно-политических целях, противоречащих международному праву, а также в террористических, экстремистских, криминальных и иных противоправных целях;

в) создание международно-правовых механизмов, учитывающих специфику информационных технологий, в целях предотвращения и урегулирования межгосударственных конфликтов в информационном пространстве;

г) продвижение в рамках деятельности международных организаций позиции Российской Федерации, предусматривающей обеспечение равноправного и взаимовыгодного сотрудничества всех заинтересованных сторон в информационной сфере;

д) развитие национальной системы управления российским сегментом сети "Интернет".

#### V. Организационные основы обеспечения информационной безопасности

30. Система обеспечения информационной безопасности является частью системы обеспечения национальной безопасности Российской Федерации.

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.

31. 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.

32. Состав системы обеспечения информационной безопасности определяется Президентом Российской Федерации.

33. 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.

34. Деятельность государственных органов по обеспечению информационной безопасности основывается на следующих принципах:

а) законность общественных отношений в информационной сфере и правовое равенство всех участников таких отношений, основанные на конституционном праве граждан свободно искать, получать, передавать, производить и распространять информацию любым законным способом;

б) конструктивное взаимодействие государственных органов, организаций и граждан при решении задач по обеспечению информационной безопасности;

в) соблюдение баланса между потребностью граждан в свободном обмене информацией и ограничениями, связанными с необходимостью обеспечения национальной безопасности, в том числе в информационной сфере;

г) достаточность сил и средств обеспечения информационной безопасности, определяемая в том числе посредством постоянного осуществления мониторинга информационных угроз;

д) соблюдение общепризнанных принципов и норм международного права, международных договоров Российской Федерации, а также законодательства Российской Федерации.

35. Задачами государственных органов в рамках деятельности по обеспечению информационной безопасности являются:

а) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

б) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

в) планирование, осуществление и оценка эффективности комплекса мер по обеспечению информационной безопасности;

г) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

д) выработка и реализация мер государственной поддержки организаций, осуществляющих деятельность по разработке, производству и эксплуатации средств обеспечения информационной безопасности, по оказанию услуг в области обеспечения информационной безопасности, а также организаций, осуществляющих образовательную деятельность в данной области.

36. Задачами государственных органов в рамках деятельности по развитию и совершенствованию системы обеспечения информационной безопасности являются:

а) укрепление вертикали управления и централизация сил обеспечения информационной безопасности на федеральном, межрегиональном, региональном, муниципальном уровнях, а также на уровне объектов информатизации, операторов информационных систем и сетей связи;

б) совершенствование форм и методов взаимодействия сил обеспечения информационной безопасности в целях повышения их готовности к противодействию информационным угрозам, в том числе путем регулярного проведения тренировок (учений);

в) совершенствование информационно-аналитических и научно-технических аспектов функционирования системы обеспечения информационной безопасности;

г) повышение эффективности взаимодействия государственных органов, органов местного самоуправления, организаций и граждан при решении задач по обеспечению информационной безопасности.

37. Реализация настоящей Доктрины осуществляется на основе отраслевых документов стратегического планирования Российской Федерации. В целях актуализации таких документов Советом Безопасности Российской Федерации определяется перечень приоритетных направлений обеспечения информационной безопасности на среднесрочную перспективу с учетом положений стратегического прогноза Российской Федерации.

38. Результаты мониторинга реализации настоящей Доктрины отражаются в ежегодном докладе Секретаря Совета Безопасности Российской Федерации Президенту Российской Федерации о состоянии национальной безопасности и мерах по ее укреплению.