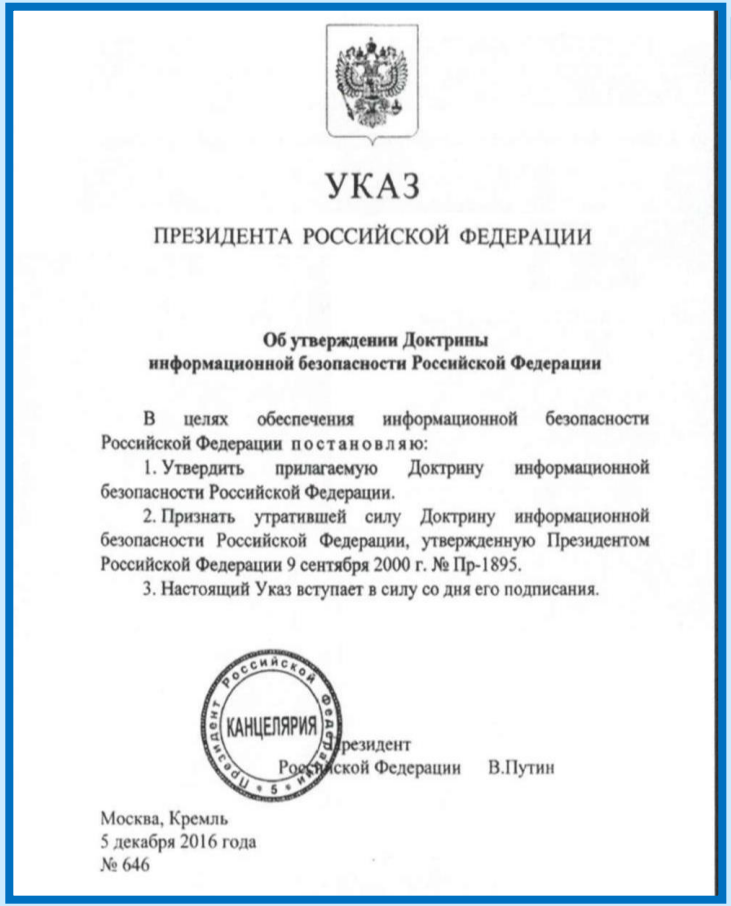
Организация защиты информации в государственных информационных системах

Доктрина информационной безопасности Российской Федерации



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. № Пр-1895.

3. Настоящий Указ вступает в силу со дня его подписания.

Президент Российской Федерации В.Путин

Москва, Кремль
5 декабря 2016 года
№ 646

Негативные факторы

- Наращивание рядом зарубежных стран возможностей информационно-технического воздействия на информационную инфраструктуру в военных целях
- **Усиление деятельности организаций, осуществляющих техническую разведку в отношении российских государственных органов, научных организаций и предприятий ОПК**
- Расширение масштабов использования специальными службами отдельных государств средств оказания информационно-психологического воздействия
- Возрастание масштабов компьютерной преступности
- Увеличение масштабов применения отдельными государствами и организациями информационных технологий в военно-политических целях

Правовая основа развития информатизации в Российской Федерации

Стратегия развития информационного общества в Российской Федерации на 2017 - 2030 годы
(Указ Президента РФ от 9 мая 2017 г. № 203)

Стратегия развития отрасли информационных технологий в Российской Федерации на 2014-2020 годы и на перспективу до 2025 года
(распоряжение Правительства РФ от 1 ноября 2013 г. № 2036-р)

Концепция развития механизмов предоставления государственных и муниципальных услуг в электронном виде
(распоряжение Правительства РФ от 25 декабря 2013 г. № 2516-р)

Концепция региональной информатизации
(распоряжение Правительства РФ от 29 декабря 2014 г. № 2769-р

Концепция перевода обработки и хранения государственных информационных ресурсов, не содержащих сведения, составляющие государственную тайну, в систему федеральных и региональных центров обработки данных
(распоряжение Правительства РФ от 7 октября 2015 г. № 1995-р)

Система нормативных правовых актов и методических документов ФСТЭК России по защите информации в ГИС

ТРЕБОВАНИЯ
о защите информации, не составляющей государственную тайну, содержащейся в ГИС

Утверждены приказом ФСТЭК России от 11.02.2013 № 17

МЕРЫ
защиты информации в государственных информационных системах

Утверждены ФСТЭК России 11.02.2014

ТРЕБОВАНИЯ
к системам обнаружения вторжений
(приказ ФСТЭК России от 6.12.2011 № 638)

ТРЕБОВАНИЯ
к средствам антивирусной защиты
(приказ ФСТЭК России от 20.03.2012 № 28

ТРЕБОВАНИЯ
к средствам доверенной загрузки
(приказ ФСТЭК России от 27.09.2013 № 119)

ТРЕБОВАНИЯ
к средствам контроля съемных машинных носителей информации
(приказ ФСТЭК России от 28.07.2014 № 87)

ТРЕБОВАНИЯ
безопасности информации к операционным системам

(приказ ФСТЭК России от 19 августа 2016 г. № 119)

ТРЕБОВАНИЯ
к межсетевым экранам
(приказ ФСТЭК России от 9 февраля 2016 г. № 9)

Изменения Требований о защите информации

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**

ПРИКАЗ
от 15 февраля 2017 г. № 27

О внесении изменений в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17

**ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ
И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)**

ПРИКАЗ
от 23 марта 2017 г. № 49

О внесении изменений в Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом ФСТЭК России от 18 февраля 2013 г. № 21, и в Требования к обеспечению защиты информации в АСУ ТП на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом ФСТЭК России от 14 марта 2014 г. № 31

Основные изменения Требований…, утвержденных приказом ФСТЭК России от 11 февраля 2013 г. № 17

Установлены 3 класса защищенности ИС ***(самый низкий – 3, самый высокий - 1)***

Для определения угроз безопасности информации обязателен к использованию банк данных угроз безопасности информации (bdu.fstec.ru)

Запрет на проведение аттестационных испытаний ИС, должностными лицами, проектирующими и (или) внедряющими системы защиты информации ИС

Определены методы проведения аттестационных испытаний
(экспертно-документальный, анализ уязвимостей ИС и испытания системы защиты информации)

Установлен предельный срок действия аттестата соответствия – 5 лет

Определен порядок аттестации ИС, функционирующих на базе общей инфраструктуры, а также на базе центра обработки данных

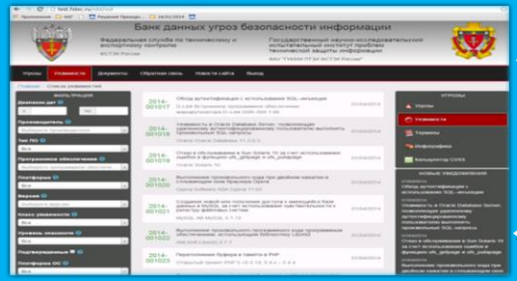
Унифицированы требования к классам защиты средств защиты информации применительно к классам защищенности ИС

Установлены формы сертификации применяемых средств защиты информации ***(на соответствие обязательным требованиям, установленными ФСТЭК России или указанным в технических условиях (заданиях по безопасности)***

Банк данных угроз безопасности информации

Банк угроз

Веб-сайт в сети Интернет



Органы государственной власти, организации

Физические лица

По состоянию на 16.06.2017 :

202 угрозы безопасности информации

16 543 уязвимости информационных технологий

Распределение уязвимостей по уровням опасности