



**Основные направления совершенствования  
Системы сертификации  
средств защиты информации**

# Нормативная правовая база по сертификации средств защиты информации

**Закон от 21.07.1993 № 5485-1  
«О государственной тайне»**

*Ст. 28. Средства защиты информации должны иметь **сертификат**, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.  
Организация сертификации средств защиты информации возлагается на ФСТЭК России...*



**Постановление Правительства РФ от 26.06.1995 № 608  
«О сертификации средств защиты информации»**

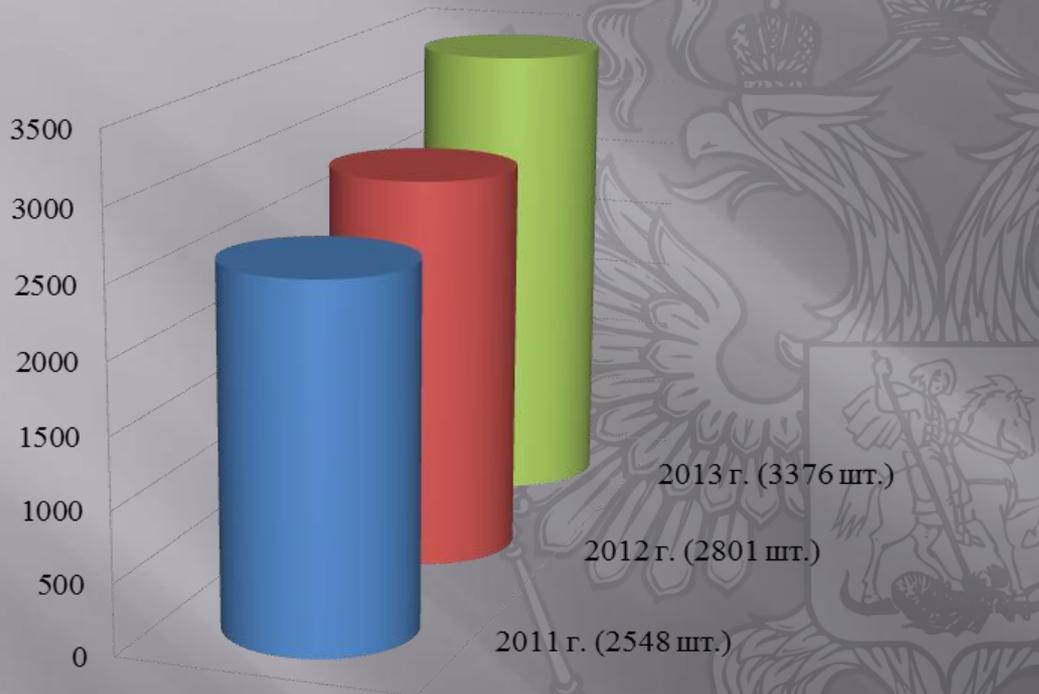
*Пункт 2. Государственной технической комиссии при Президенте Российской Федерации в пределах определенной законодательством Российской Федерации компетенции в 3-месячный срок разработать и ввести в действие соответствующее положение о системе сертификации*



**Положение о сертификации средств защиты информации по требованиям безопасности информации, утвержденное приказом председателя Государственной технической комиссии при Президенте Российской Федерации от 27.10.95 № 199**

# ОСНОВНЫЕ ПОКАЗАТЕЛИ ДЕЯТЕЛЬНОСТИ СИСТЕМЫ СЕРТИФИКАЦИИ ФСТЭК РОССИИ

Динамика роста количества сертифицированных средств защиты информации



Выдано **более 3000** сертификатов соответствия

С 2005 г. выдано **8,5 млн.** знаков соответствия для маркирования средств защиты информации

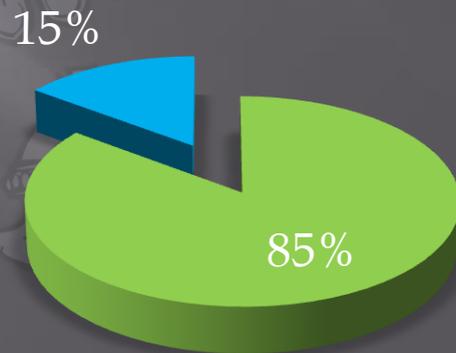
Участники Системы сертификации

**9** органов по сертификации

**43** испытательных лабораторий

**450** органов по аттестации

**300** заявителей на сертификацию



■ СЗИ от НСД

■ СЗИ от утечки по ТК

## Направления совершенствования Системы сертификации ФСТЭК России

**1. Совершенствование организации и порядка проведения сертификации средств защиты информации.**

**2. Разработка требований к средствам защиты информации.**

**3. Совершенствование методических подходов по сертификации средств защиты информации.**

**4. Совершенствование аттестации объектов информатизации по требованиям безопасности информации**

# 1. Совершенствование организации и порядка проведения сертификации СЗИ

Постановление Правительства Российской Федерации от 15 мая 2010 г. № 330 «Об утверждении Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну...»



Проект нормативного правового акта ФСТЭК России «Организация и порядок проведения сертификации продукции, используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну»  
(утверждение планируется в 2014 году)

# Задачи, которые планируется решить в НПА «Организация и порядок проведения сертификации...»

Детализация  
порядка  
сертификации  
СЗИ с  
установлением  
сроков  
выполнения её  
отдельных  
процедур

Отмена  
процедуры  
продления  
срока действия  
сертификата  
соответствия на  
СЗИ для  
потребителей

Установление  
порядка  
проведения  
инспекционного  
контроля СЗИ,  
связанного с их  
обновлением

## 2. Разработка требований к средствам защиты информации от несанкционированного доступа

**Статья 5 Федерального закона от 21 декабря 2002 г.**

**№184-ФЗ «О техническом регулировании»**

в отношении продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа обязательными требованиями наряду с требованиями технических регламентов являются требования, установленные уполномоченными федеральными органами исполнительной власти, в том числе ФСТЭК России

**Подпункт 13.1 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085**

ФСТЭК России разрабатывает и устанавливает в пределах своей компетенции обязательные требования в области технического регулирования к продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, издает по данному вопросу нормативные правовые акты; разрабатывает и утверждает методические документы

## 2.1. Разработка требований к средствам защиты информации от НСД

Требования к системам обнаружения вторжений, утверждены приказом ФСТЭК России от 6 декабря 2011 г. N 638, зарегистрирован Минюстом России 1 февраля 2012 г., рег. N 23088.

12 методических документа, устанавливающих профили защиты к системам обнаружения вторжений.

Требования к средствам антивирусной защиты, утверждены приказом ФСТЭК России от 20 марта 2012 г. N 28, зарегистрирован Минюстом России 3 мая 2012 г., рег. N 24045.

24 методических документа, устанавливающих профили защиты к средствам антивирусной защиты.

Требования к средствам доверенной загрузки, утверждены приказом ФСТЭК России от 27 сентября 2013 г. N 119, зарегистрирован Минюстом России 16 декабря 2013 г., рег. N 30604.

10 методических документов, устанавливающих профили защиты к средствам доверенной загрузки.

## 2.1. Разработка требований к средствам защиты информации от НСД

### В 2014 году планируются к утверждению:

1. Требования к средствам контроля съемных носителей информации.
2. Требования к средствам межсетевое экранирования.
3. Требования к средствам управления потоками информации (коммутационное оборудование с встроенными механизмами защиты, средства однонаправленной передачи информации).
4. Требования к средствам аутентификации.
5. Требования к DLP-системам.
6. Требования к средствам контроля и анализа защищенности.

### В 2015 году планируются к утверждению:

1. Требования к средствам разграничения доступа.
2. Требования к средствам контроля целостности.
3. Требования к средствам очистки памяти.
4. Требования к средствам ограничения программной среды.
5. Требования к средствам защиты среды виртуализации

## 2.1. Разработка требований к средствам защиты информации от НСД

Требования к СЗИ предназначены для:

- разработчиков и производителей СЗИ
- заявителей на сертификацию СЗИ
- испытательных лабораторий
- органов по сертификации

Требования к СЗИ включают:

1. Общие требования
2. Требования к функциям безопасности
  - требования к составу реализуемых функций СЗИ безопасности и сред, в которых они функционируют;
  - требования к составу функциональных возможностей СЗИ;
  - требования к реализации функциональных возможностей СЗИ;
  - требования доверия к безопасности СЗИ.

## 2.2. Разработка требований к средствам защиты информации от НСД

В 2014 году планируется утвердить методический документ ФСТЭК России «Рекомендации по обновлению сертифицированных средств защиты информации»

В 2015 году планируется представить на утверждение в Росстандарт проект национального стандарта ГОСТ РXXXXXX-20XX «Защита информации. Разработка безопасных программных средств. Требования»

## 2.1. Разработка требований к средствам защиты информации от НСД

### Классификация СЗИ

Для дифференциации требований к функциям безопасности СЗИ выделяются 6 классов защиты СЗИ. Самый низкий класс - 6, самый высокий – 1.

**СЗИ 6 класса защиты** применяются в ИС, не являющихся ГИС, ИСПДн, ИСОП и не предназначенных для обработки сведений, содержащих государственную тайну.

**СЗИ 5 класса защиты**, применяются в ГИС 3 класса защищенности в случае отсутствия взаимодействия ГИС с информационно-телекоммуникационными сетями международного информационного обмена, а также в ГИС 4 класса защищенности, в ИСПДн при необходимости обеспечения 3 уровня защищенности ПДн в случае актуальности угроз 3-го типа и отсутствия взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 4 уровня защищенности ПДн.

**СЗИ 4 класса защиты**, применяются в ГИС 3 класса защищенности в случае их взаимодействия с информационно-телекоммуникационными сетями международного информационного обмена, а также в ГИС 1 и 2 классов защищенности, в ИСПДн при необходимости обеспечения 3 уровня защищенности ПДн в случае актуальности угроз 2-го типа или взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена, а также при необходимости обеспечения 1 и 2 уровня защищенности ПДн, в ИСОП II класса.

## 2.2. Разработка требований к средствам защиты информации от утечки по техническим каналам

**В 2014...2015 годах планируются к утверждению:**

1. Требования к средствам активной защиты информации от утечки по каналам ПЭМИН.
2. Требования к средствам виброакустической защиты информации.
3. Требования к ПЭВМ защищенным от утечки информации по каналам ПЭМИН.
4. Требования к средствам пассивной защиты информации от утечки по каналам ПЭМИН.
5. Требования к средствам защиты информации от акустоэлектрических преобразований.

### 3. Совершенствование методических подходов по сертификации средств защиты информации

С 2014 года ФСТЭК России планируется утверждение методических документов, устанавливающих

**Типовые программы и методики сертификационных испытаний СЗИ**



**Типовые программы и методики сертификационных испытаний СЗИ обеспечат:**

повышение качества проведения сертификационных испытаний СЗИ

единство подходов при проведении сертификационных испытаний СЗИ

воспроизводимость результатов сертификационных испытаний СЗИ

## 4. Совершенствование аттестации объектов информатизации по требованиям безопасности информации

ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения», утвержден приказом Федерального агентства по техническому регулированию и метрологии от 17 апреля 2012 г. № 2-СТ РО

ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний» утвержден приказом Федерального агентства по техническому регулированию и метрологии от 12 апреля 2013 г. № 1-СТ РО

**проект ГОСТ Р XXXX-XXX-201X «Защита информации. Документация по технической защите информации на объекте информатизации. Общие положения» (планируется представить на утверждение в Росстандарт в 2014 году.)**

**разрабатывается методический документ «Порядок аттестации распределенных государственных информационных систем» (планируется к утверждению в 2015 г.)**



Спасибо за внимание !