



# ТЕХНИЧЕСКОЕ РЕГУЛИРОВАНИЕ И СТАНДАРТИЗАЦИЯ В ОБЛАСТИ ИКТ

- **Обеспечение качества и безопасности процессов, продукции и услуг в сфере информационных технологий, требований международных стандартов серии ИСО 9000 в части создания систем менеджмента качества, структуры и основных требований национальных и международных стандартов в сфере средств информационных технологий.**

- Для правильного представления места и роли стандартизации в области ИКТ, необходимо дать определение этому понятию как объекту стандартизации.

ИКТ – совокупность методов, производственных процессов и промышленно-технических средств, объединенных в технологическую цепочку с целью сбора, обработки, хранения, распространения, отображения и использования информации в интересах ее пользователей.

- Основными направлениями стандартизации в области ИКТ являются:
- системы автоматической обработки текстов и речи расчетно-логические и эксплуатационные системы
- системы автоматической обработки текстов и речи интеллектуальные системы для использования в управлении, проектировании, обучении и т. д.;
- CALS-технологии непрерывной информационной поддержки ЖЦП
- Стандартизацией ИКТ на международном уровне занимаются три международные организации ISO, IEC, ITU.
- ISO (ИСО) (International Organization for Standardization - Международная организация стандартизации)
- IEC (МЭК) (International Electrotechnical Commission - Международная электротехническая комиссия)
- ITU (МСЭ) (International Telecommunication Union - Международный союз электросвязи,)

- ISO и IEC, а также их совместным техническим комитетом по стандартизации SO/IEC/JTC1 разработано более 1500 международных стандартов, охватывающих следующие области ИКТ:
  - телекоммуникационный и информационный обмен между системами
  - компьютерная графика и обработка изображения программное обеспечение
  - безопасность информационных технологий средства для цифрового обмена данными
  - автоматический сбор данных идентификационные карточки
  - управление использованием данных
  - языки программирования, их среда и интерфейс программного обеспечения
  - описание документа и языковая обработка совместимость
  - информационно технологического оборудования пользовательский интерфейс и т.д.

- Альтернативой международным консорциумам является деятельность большого числа конкурирующих компаний (HP, IBM, Sun Microsystems, SCO Group, Novell др.), производящих совместимую серийную технику, стандарты которой становятся международными «дефакто» (в международной практике – одна из форм признания, означающая официальное, но еще не юридическое признание).



- Работы по стандартизации ИКТ также проводятся промышленными профессиональными организациями, среди которых следует особо выделить Институт инженеров по электротехнике и электронике (IEEE).
- Первый стандарт по разработке программного обеспечения был создан IEEE еще в 1979 г. К 1990 г.

- ISO/IEC JTC 1/SC 7 разработал 8 стандартов (6 действуют и в настоящее время), IEEE к этому времени уже разработал 14 стандартов по программному обеспечению, число которых возросло до 27 к 1994 г., сейчас их более 50.
- На региональном уровне в странах ЕС координацию работы по стандартизации и обеспечению качества ИКТ проводят: Европейский комитет по стандартизации (CEN), Европейский комитет по стандартизации в электротехнике (CENELEC), Европейский институт по стандартизации в области электросвязи (ETSI).



- Европейский комитет по стандартизации (фр. Comité Européen de Normalisation, CEN) — международная некоммерческая организация, основной целью которой является содействие развитию торговли товарами и услугами путём разработки европейских стандартов (евронорм, EN).
- Основная ETSI задача — поиск общих стандартов, на основе которых можно создать комплексную инфраструктуру электросвязи. Эта инфраструктура призвана обеспечить полную совместимость любого оборудования и услуг, предлагаемых потребителям.

Кроме указанных организаций в работе по созданию стандартов ИКТ участвуют и специализированные региональные организации, которыми разработано более 600 европейских стандартов в области ИКТ:

- 1. Европейская конференция почтовой и телеграфной связи (CEPT) (CEPT была образована в 1959 году 19 странами. В настоящее время включает в себя 48 стран-членов, охватывая практически всю Европу)
- 2. Европейский комитет по сертификации в области информационных технологий (ECITS).



# СТАНДАРТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РФ

- Основным направлением работ по стандартизации ИКТ в РФ является использование международных достижений и принятие международных стандартов в качестве государственных.
- Информационная безопасность – состояние защищенности информационной среды общества, обеспечивающее формирование, использование и развитие в интересах граждан, организаций, государства.

Защита информации представляет собой деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию, т. е. процесс, направленный на достижение этого состояния. В качестве стандартной модели безопасности часто используется модель CIA:

- С – конфиденциальность (confidentiality) – доступность информации только определенному кругу лиц;
- – I – целостность (integrity) – гарантия существования информации в исходном виде;
- – A – доступность (availability) – возможность получения информации авторизованным пользователем в нужное для него время.

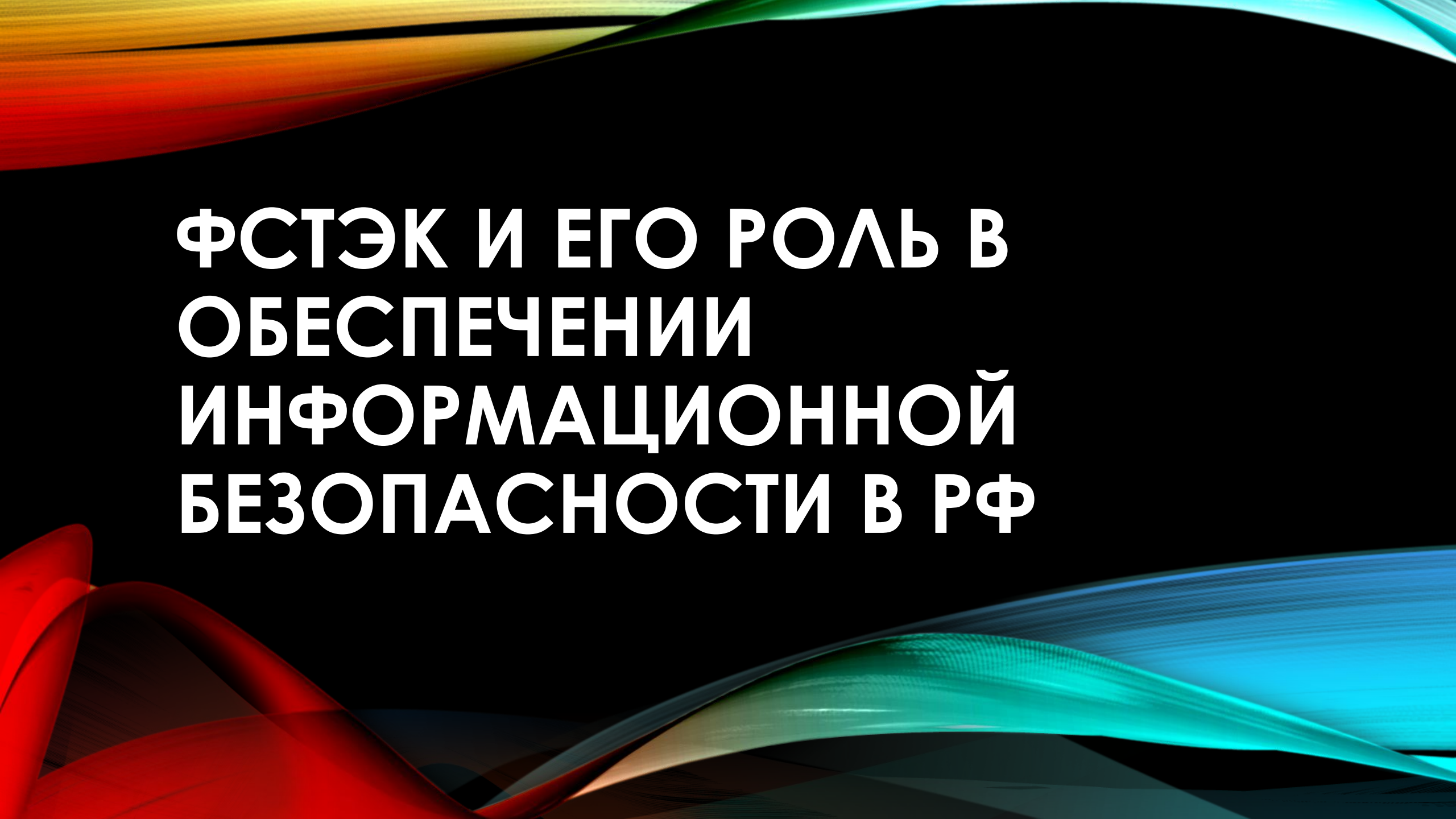


К перечисленным выше можно добавить и другие категории информационной безопасности:

- аутентичность – возможность установления автора информации;

- апеллируемость – возможность доказать, что автором является именно заявленный человек, а не другой.





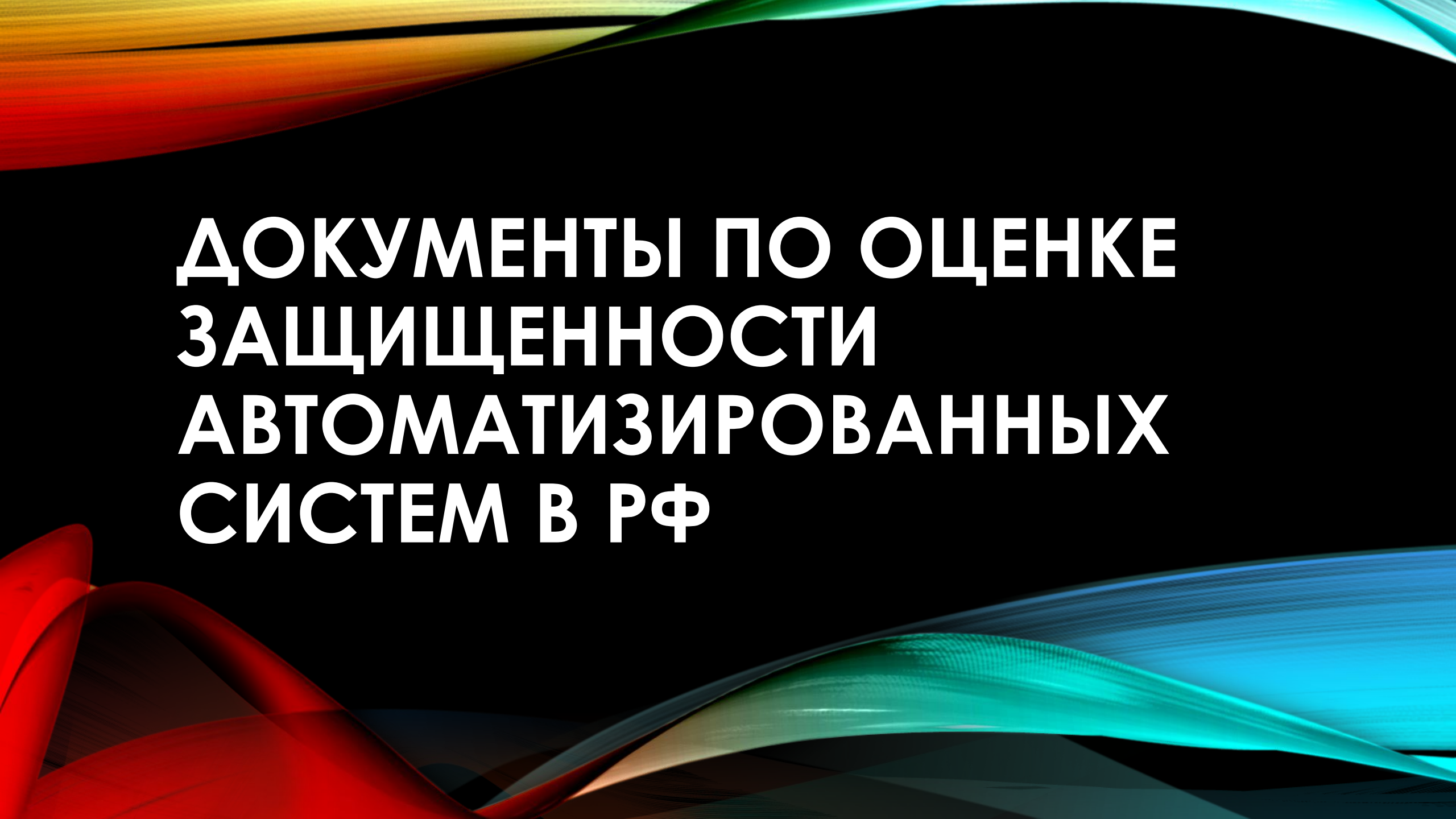
**ФСТЭК И ЕГО РОЛЬ В  
ОБЕСПЕЧЕНИИ  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ В РФ**

- В Российской Федерации информационная безопасность обеспечивается соблюдением указов Президента, федеральных законов, постановлений Правительства Российской Федерации, руководящих документов ФСТЭК России и других нормативных документов. В РФ с точки зрения стандартизации положений в сфере информационной безопасности первостепенное значение имеют руководящие документы (РД) ФСТЭК России, одной из задач которой является "проведение единой государственной политики в области технической защиты информации". ФСТЭК России ведет весьма активную нормотворческую деятельность, выпуская руководящие документы, играющие роль национальных оценочных стандартов в области информационной безопасности.

В качестве стратегического направления ФСТЭК России выбрала ориентацию на "Общие критерии".

- За 15 лет своего существования ФСТЭК разработала и довела до уровня национальных стандартов десятки документов, среди которых:
- Руководящий документ "Положение по аттестации объектов информатизации по требованиям безопасности информации" (Утверждено Председателем ФСТЭК России 25.11.1994 г.).
- Руководящий документ "Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации" (ФСТЭК России, 1997 г.).

- Руководящий документ "Средства вычислительной техники. Защита от НСД к информации. Показатели защищенности от НСД к информации" (ФСТЭК России, 1992 г.).  
Руководящий документ "Концепция защиты средств вычислительной техники от НСД к информации" (ФСТЭК России, 1992 г.).
- Руководящий документ "Защита от НСД к информации. Термины и определения" (ФСТЭК России, 1992 г.).
- Руководящий документ "Средства вычислительной техники (СВТ). Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации" (ФСТЭК России, 1997 г.).
- Руководящий документ "Специальные требования и рекомендации по технической защите конфиденциальной информации" (ФСТЭК России, 2001 г.).



**ДОКУМЕНТЫ ПО ОЦЕНКЕ  
ЗАЩИЩЕННОСТИ  
АВТОМАТИЗИРОВАННЫХ  
СИСТЕМ В РФ**



- Руководящий документ "СВТ. Защита от НСД к информации.  
Показатели защищенности от НСД к информации" устанавливает классификацию СВТ по уровню защищенности от НСД к информации на базе перечня показателей защищенности и совокупности описывающих их требований.
- Основой для разработки этого документа явилась "Оранжевая книга". Этот оценочный стандарт устанавливается семь классов защищенности СВТ от НСД к информации.



Самый низкий класс – седьмой, самый высокий – первый.

Классы подразделяются на четыре группы, отличающиеся уровнем защиты:

- I. первая группа содержит только один седьмой класс, к которому относят все СВТ, не удовлетворяющие требованиям более высоких классов;
- II. вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- III. третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- IV. четвертая группа характеризуется верифицированной защитой и включает только первый класс.

- Руководящий документ "АС. Защита от НСД к информации. Классификация АС и требования по защите информации" устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

- I. наличие в АС информации различного уровня конфиденциальности;
- II. уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;
- III. режим обработки данных в АС – коллективный или индивидуальный.

В документе определены девять классов защищенности АС от НСД к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности и конфиденциальности информации и, следовательно, иерархия классов защищенности АС.