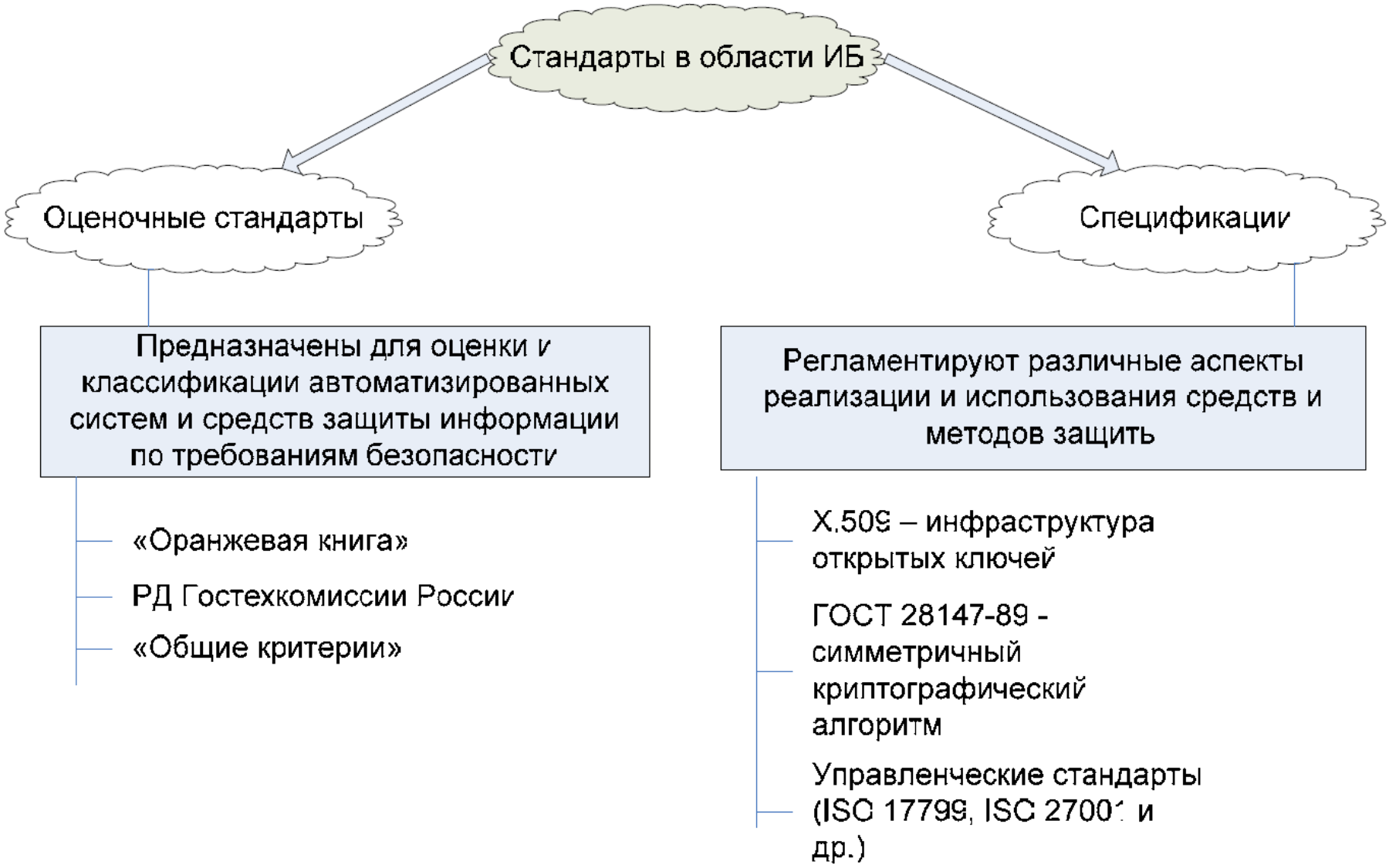
Стандарты в информационной безопасности

- Стандарт - документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт может задавать и другие требования – например, к символике или терминологии.

Классификация стандартов в области ИБ



- Руководящие документы (РД) Гостехкомиссии России действуют и активно используются при проведении сертификации средств защиты информации в системах сертификации ФСТЭК России, Минобороны России, а также в ряде добровольных систем сертификации.
- Стандарт ГОСТ Р ИСО/МЭК 15408-2002, более известный как «Общие критерии», действует и применяется при проведении сертификации средств защиты, не предназначенных для работы с информацией, составляющей государственную тайну. В перспективе предполагается отказ от РД Гостехкомиссии России и полноценный переход к «Общим критериям» как единому оценочному стандарту.
- Криптографические стандарты (ГОСТ 28147-89, ГОСТ 3410-2001, ГОСТ 3411-94) являются обязательными для применения в системах защиты информации, позиционируемых как средства криптографической защиты.
- Управленческие стандарты ISO 17799-2005 и ISO 27001-2005 в настоящее время не имеют в РФ официального статуса.

«Оранжевая книга»

Стандарт «Критерии оценки доверенных компьютерных систем» (Trusted Computer System Evaluation Criteria), более известный как «Оранжевая книга», был разработан Министерством Обороны США в 1983 г. и стал первым в истории общедоступным оценочным стандартом в области информационной безопасности.

- Структура требований:

1. Политика безопасности:
    1. Система должна поддерживать точно определенную политику безопасности. Возможность доступа субъектов к объектам должна определяться на основании их идентификации и набора правил управления доступом. По мере необходимости должна использоваться политика мандатного управления доступом.
    2. С объектами должны быть ассоциированы метки безопасности, используемые в качестве исходной информации для процедур контроля доступа. Для реализации мандатного управления доступом система должна обеспечивать каждому объекту набор атрибутов, определяющих степень конфиденциальности объекта и режимы доступа к этому объекту.

2. Подотчетность

1. Все субъекты должны имеет уникальные идентификаторы. Контроль доступа должен осуществляться на основе идентификации субъекта и объекта доступа, аутентификации и правил разграничения доступа. Данные, используемые для идентификации и аутентификации, должны быть защищены от несанкционированного доступа, модификации и уничтожения и должны быть ассоциированы со всеми активными компонентами компьютерной системы, функционирование которых критично сточки зрения безопасности.
2. Для определения степени ответственности пользователя за действия в системе, все происходящие в ней события, имеющие значение сточки зрения безопасности, должны отслеживаться и регистрироваться в защищённом протоколе. Система регистрации должна осуществлять анализ общего потока событий и выделят из него только те события, которые оказывают влияние на безопасность. Протокол событий должен быть надёжно защищён от несанкционированного доступа, модификации и уничтожения.

3. Гарантии

1. Средства защиты должны содержать независимые аппаратные или программные компоненты, обеспечивающие работоспособность функций защиты. Это означает, что все средства защиты, обеспечивающие политику безопасности, управление атрибутами и метками безопасности, регистрацию и учёт, должны находиться под контролем средств, проверяющих корректность их функционирования. Средства контроля должны быть полностью независимы от средств защиты.
2. Все средства защиты должны быть защищены от несанкционированного вмешательства и отключения, причём эта защита должна быть постоянной и непрерывной в любом режиме функционирования системы защиты и автоматизированной системы в целом. Данное требование распространяется на весь жизненный цикл автоматизированной системы.

Классы защищенности

- A – содержит единственный класс A1.
- B – содержит классы B1, B2 и B3.
- C – содержит классы C1 и C2.
- D – содержит единственный класс D1.

- Требуемый уровень защищённости системы возрастает от группы D к группе A, а в пределах одной группы – с увеличением номера класса. Каждый класс характеризуется определённым фиксированным набором требований к подсистеме обеспечения информационной безопасности, реализованной в АС.

Краткие характеристики классов

I. Группа D – минимальная защита.

К данной категории относятся те системы, которые были представлены для сертификации по требованиям одного из более высоких классов защищённости, но не прошли испытания.

II. Группа C - дискреционная защита.

Данная группа характеризуется наличием дискреционного управления доступом и регистрации действий субъектов.

- **Класс C1 – дискреционная защита**: Система включает в себя средства контроля и управления доступом, позволяющие задавать ограничения для отдельных пользователей. Класс C1 рассчитан на однопользовательские системы, в которых осуществляется совместная обработка данных одного уровня конфиденциальности.
- **Класс C2 – управление доступом**: Система обеспечивает более избирательное управление доступом путём применения средств индивидуального контроля за действиями пользователей, регистрации, учёта событий и выделения ресурсов.

III. Группа В – мандатная защита. Система обеспечивает мандатное управление доступом с использованием меток безопасности, поддержку модели и политики безопасности. Предполагается наличие спецификаций на функции ядра безопасности. Реализуется концепция монитора безопасности обращений, контролирующего все события в системе.

- **Класс В1 – защита с применением меток безопасности**: Помимо выполнения всех требований к классу С2, система должна поддерживать маркировку данных и мандатное управление доступом. При экспорте из системы информация должна подвергаться маркировке.
- **Класс В2 – структурированная защита**: Ядро безопасности должно поддерживать формально определённую и чётко документированную модель безопасности, предусматривающую дискреционное и мандатное управление доступом, которое распространяется на все субъекты. Должен осуществляться контроль скрытых каналов передачи информации. В структуре ядра безопасности должны быть выделены элементы, критичные с точки зрения безопасности. Интерфейс ядра безопасности должен быть чётко определён, а его архитектура и реализация должны быть выполнены с учётом возможности проведения тестовых испытаний. Управление безопасностью должно осуществляться администратором безопасности.

- **Класс B3 – домены безопасности**: Ядро безопасности должно поддерживать монитор безопасности обращений, который контролирует все типы доступа субъектов к объектам и который невозможно обойти. Ядро безопасности содержит исключительно подсистемы, отвечающие за реализацию функций защиты, и является достаточно компактным для обеспечения возможности эффективного тестирования. Средства аудита должны включать механизмы оповещения администратора о событиях, имеющих значение для безопасности системы. Необходимо наличие средств восстановления работоспособности системы.

IV. Группа А – верифицированная защита

Группа характеризуется применением формальных методов верификации корректности функционирования механизмов управления доступом. Требуется дополнительная документация, демонстрирующая, что архитектура и реализация ядра безопасности отвечает требованиям безопасности. Функциональные требования совпадают с классом B3, однако на всех этапах разработки АС требуется применение формальных методов верификации систем защиты.

Руководящие документы ФСТЭК России

- ФСТЭК – Федеральная служба по техническому и экспортному контролю.
- Перечень необходимых документов:
  - Защита от несанкционированного доступа к информации. Термины и определения.
  - Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации.
  - Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.
  - Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации.
  - Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа. Показатели защищённости от несанкционированного доступа к информации.
  - Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей.

Темы докладов

- Управление доступом
- Подделка документов
- Комплексные меры по защите информации
- Преодоление защиты информации
- Электронная подпись
- Защита информации личного характера
- Информационная безопасность
- Средства обеспечения информационной безопасности
- История возникновения и развития информационной безопасности
- Правонарушения в области защищенных систем
- Практические меры защиты информации
- Программы с потенциально опасными последствиями (Вирусы).
- Управление безопасностью
- Лицензирование и сертификация в области защиты информации