СТАНДАРТЫ И СПЕЦИФИКАЦИИ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Виды стандартов и спецификаций

- оценочные стандарты, направленные на классификацию информационных систем и средств защиты по требованиям безопасности;
- технические спецификации, регламентирующие различные аспекты реализации средств защиты.

Оранжевая книга

Исторически первым оценочным стандартом, получившим широкое распространение и оказавшим огромное влияние на базу стандартизации ИБ во многих странах, стал стандарт Министерства обороны США "Критерии оценки доверенных компьютерных систем ".

Данный труд, называемый чаще всего по цвету обложки "Оранжевой книгой", был впервые опубликован в августе 1983 года.

Доверие к системам оцениваются исключительно с точки зрения управления доступом к данным, что является одним из средств обеспечения конфиденциальности и целостности. Вопросы доступности "Оранжевая книга" не затрагивает.

Оранжевая книга

Безопасная система управляет, с помощью соответствующих средств, доступом к информации так, что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать, создавать и удалять информацию.

Абсолютно безопасных систем не существует, это абстракция. Есть смысл оценивать лишь степень доверия, которое можно оказать той или иной системе.

Доверенная система – это система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа.

Критерии оценки степени доверия

Политика безопасности - набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. Чем выше степень доверия системе, тем строже и многообразнее должна быть политика безопасности. В зависимости от сформулированной политики можно выбирать конкретные механизмы обеспечения безопасности. Политика безопасности - это активный аспект защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Уровень гарантированности - мера доверия, которая может быть оказана архитектуре и реализации ИС. Доверие безопасности может проистекать как из анализа результатов тестирования, так и из проверки (формальной или нет) общего замысла и реализации системы в целом и отдельных ее компонентов. Уровень гарантированности показывает, насколько корректны механизмы, отвечающие за реализацию политики безопасности. Это пассивный аспект защиты.

Оранжевая книга

Доверенная вычислительная база - это совокупность защитных механизмов ИС (включая аппаратное и программное обеспечение), отвечающих за проведение в жизнь политики безопасности. Качество вычислительной базы определяется исключительно ее реализацией и корректностью исходных данных, которые вводит системный администратор. Основное назначение – выполнять функции **монитора обращений**, то есть контролировать допустимость выполнения субъектами (активными сущностями ИС, действующими от имени пользователей) определенных операций над объектами (пассивными сущностями). Монитор проверяет каждое обращение пользователя к программам или данным на предмет согласованности с набором допустимых действий.

Границу доверенной вычислительной базы называют **периметром безопасности**. Сейчас этому понятию все чаще придают другой смысл, имея в виду границу владений определенной организации. То, что находится внутри владений, считается доверенным, а то, что вне, - нет.

Монитор обращений

Монитор обращений должен обладать тремя качествами:

- Изолированность. Необходимо предупредить возможность отслеживания работы монитора.
- Полнота. Монитор должен вызываться при каждом обращении, не должно быть способов обойти его.
- Верифицируемость. Монитор должен быть компактным, чтобы его можно было анализировать и протестировать, будучи уверенным в полноте тестирования.

Реализация монитора обращений называется ядром безопасности. Ядро безопасности - это основа, на которой строятся все защитные механизмы. Ядро должно гарантировать собственную неизменность.

Механизмы безопасности

Согласно "Оранжевой книге", политика безопасности должна обязательно включать в себя следующие элементы:

- произвольное управление доступом;
- безопасность повторного использования объектов;
- метки безопасности;
- принудительное управление доступом.

Механизмы безопасности

Произвольное управление доступом (или дискреционное) - это метод разграничения доступа к объектам, основанный на учете личности субъекта или группы, в которую субъект входит. Произвольность управления состоит в том, что некоторое лицо (обычно владелец объекта) может по своему усмотрению предоставлять другим субъектам или отбирать у них права доступа к объекту.

Безопасность повторного использования объектов - механизм, предохраняющий от случайного или преднамеренного извлечения конфиденциальной информации из "мусора". Безопасность повторного использования должна гарантироваться для областей оперативной памяти (в частности, для буферов с образами экрана, расшифрованными паролями и т.п.), для дисковых блоков и магнитных носителей в целом.

Монитор обращений

Для реализации **принудительного управления доступом** с субъектами и объектами ассоциируются **метки безопасности**. Метка субъекта описывает его благонадежность, метка объекта - степень конфиденциальности содержащейся в нем информации.

Согласно "Оранжевой книге", **метки безопасности** состоят из двух частей - уровня секретности и списка категорий. Назначение последних - описать предметную область, к которой относятся данные. **Принудительное (или мандатное) управление доступом** основано на сопоставлении меток безопасности субъекта и объекта.

Принудительное управление доступом

Субъект может читать информацию из объекта, если уровень секретности субъекта не ниже, чем у объекта, а все категории, перечисленные в метке безопасности объекта, присутствуют в метке субъекта. В таком случае говорят, что метка субъекта доминирует над меткой объекта. Смысл сформулированного правила понятен - читать можно только то, что положено.

Субъект может записывать информацию в объект, если метка безопасности объекта доминирует над меткой субъекта. В частности, "конфиденциальный" субъект может записывать данные в секретные файлы, но не может - в несекретные.

Механизм подотчетности

Цель подотчетности - в каждый момент времени знать, кто работает в системе и что делает. Средства подотчетности делятся на три категории:

- идентификация и аутентификация;
- предоставление доверенного пути;
- анализ регистрационной информации.

Механизм подотчетности

Обычный способ **идентификации** - ввод имени пользователя при входе в систему. Стандартное средство проверки подлинности (**аутентификации**) пользователя - пароль.

Доверенный путь связывает пользователя непосредственно с доверенной вычислительной базой, минуя другие, потенциально опасные компоненты ИС. Цель предоставления доверенного пути - дать пользователю возможность убедиться в подлинности обслуживающей его системы.

Анализ регистрационной информации (аудит) имеет дело с действиями (событиями), так или иначе затрагивающими безопасность системы.

Операционная и технологическая гарантированность

Операционная гарантированность - это способ убедиться в том, что архитектура системы и ее реализация действительно реализуют избранную политику безопасности. Операционная гарантированность включает в себя проверку следующих элементов:

- архитектура системы;
- целостность системы;
- проверка тайных каналов передачи информации ;
- доверенное администрирование;

Технологическая гарантированность охватывает весь жизненный цикл ИС, то есть периоды проектирования, реализации, тестирования, продажи и сопровождения.

Классы безопасности

В "Оранжевой книге" определяется четыре уровня доверия - D, C, B и A. Уровень D предназначен для систем, признанных неудовлетворительными. По мере перехода от уровня C к A к системам предъявляются все более жесткие требования. Уровни подразделяются на классы. Всего имеется шесть классов безопасности - C1, C2, B1, B2, B3, A1. Чтобы в результате процедуры сертификации систему можно было отнести к некоторому классу, ее политика безопасности и уровень гарантированности должны удовлетворять заданным требованиям, из которых далее упомянем лишь важнейшие.

Класс C1

- доверенная вычислительная база должна управлять доступом именованных пользователей к именованным объектам;
- пользователи должны идентифицировать себя, прежде чем выполнять какие-либо иные действия. Для аутентификации должен использоваться какой-либо защитный механизм, например пароли. Аутентификационная информация должна быть защищена от несанкционированного доступа;
- доверенная вычислительная база должна поддерживать область для собственного выполнения, защищенную от внешних воздействий (в частности, от изменения команд и/или данных) и от попыток слежения за ходом работы;
- должны быть в наличии аппаратные и/или программные средства, позволяющие периодически проверять корректность функционирования аппаратных и микропрограммных компонентов доверенной вычислительной базы ;
- защитные механизмы должны быть протестированы на предмет соответствия их поведения системной документации. Тестирование должно подтвердить, что у неавторизованного пользователя нет очевидных способов обойти или разрушить средства защиты доверенной вычислительной базы ;
- должны быть описаны подходы к безопасности, используемые производителем, и применение этих подходов при реализации доверенной вычислительной базы.

Класс С2 (дополнение к С1)

- права доступа должны гранулироваться с точностью до пользователя. Все объекты должны подвергаться контролю доступа;
- при выделении хранимого объекта из пула ресурсов доверенной вычислительной базы необходимо ликвидировать все следы его использования;
- каждый пользователь системы должен уникальным образом идентифицироваться. Каждое регистрируемое действие должно ассоциироваться с конкретным пользователем;
- доверенная вычислительная база должна создавать, поддерживать и защищать журнал регистрационной информации, относящейся к доступу к объектам, контролируемым базой;
- тестирование должно подтвердить отсутствие очевидных недостатков в механизмах изоляции ресурсов и защиты регистрационной информации.

Класс B1 (дополнение к C2)

- доверенная вычислительная база должна управлять метками безопасности, ассоциируемыми с каждым субъектом и хранимым объектом;
- доверенная вычислительная база должна обеспечить реализацию принудительного управления доступом всех субъектов ко всем хранимым объектам;
- доверенная вычислительная база должна обеспечивать взаимную изоляцию процессов путем разделения их адресных пространств ;
- группа специалистов, полностью понимающих реализацию доверенной вычислительной базы, должна подвергнуть описание архитектуры, исходные и объектные коды тщательному анализу и тестированию ;
- должна существовать неформальная или формальная модель политики безопасности, поддерживаемой доверенной вычислительной базой.

Класс B2 (дополнение к B1)

- снабжаться метками должны все ресурсы системы (например, ПЗУ), прямо или косвенно доступные субъектам;
- к доверенной вычислительной базе должен поддерживаться доверенный коммуникационный путь для пользователя, выполняющего операции начальной идентификации и аутентификации ;
- должна быть предусмотрена возможность регистрации событий, связанных с организацией тайных каналов обмена с памятью;
- доверенная вычислительная база должна быть внутренне структурирована на хорошо определенные, относительно независимые модули;
- системный архитектор должен тщательно проанализировать возможности организации тайных каналов обмена с памятью и оценить максимальную пропускную способность каждого выявленного канала;

Класс B2 (продолжение)

- должна быть продемонстрирована относительная устойчивость доверенной вычислительной базы к попыткам проникновения;
- модель политики безопасности должна быть формальной. Для доверенной вычислительной базы должны существовать описательные спецификации верхнего уровня, точно и полно определяющие ее интерфейс;
- в процессе разработки и сопровождения доверенной вычислительной базы должна использоваться система конфигурационного управления, обеспечивающая контроль изменений в описательных спецификациях верхнего уровня, иных архитектурных данных, реализационной документации, исходных текстах, работающей версии объектного кода, тестовых данных и документации;
- тесты должны подтверждать действенность мер по уменьшению пропускной способности тайных каналов передачи информации.

Класс B3 (дополнение к B2)

- для произвольного управления доступом должны обязательно использоваться списки управления доступом с указанием разрешенных режимов;
- должна быть предусмотрена возможность регистрации появления или накопления событий, несущих угрозу политике безопасности системы. Администратор безопасности должен немедленно извещаться о попытках нарушения политики безопасности, а система, в случае продолжения попыток, должна пресекать их наименее болезненным способом;
- доверенная вычислительная база должна быть спроектирована и структурирована таким образом, чтобы использовать полный и концептуально простой защитный механизм с точно определенной семантикой;
- процедура анализа должна быть выполнена для временных тайных каналов;
- должна быть специфицирована роль администратора безопасности. Получить права администратора безопасности можно только после выполнения явных, протоколируемых действий;
- должны существовать процедуры и/или механизмы, позволяющие произвести восстановление после сбоя или иного нарушения работы без ослабления защиты;
- должна быть продемонстрирована устойчивость доверенной вычислительной базы к попыткам проникновения.

Класс А1 (дополнение к В3)

- тестирование должно продемонстрировать, что реализация доверенной вычислительной базы соответствует формальным спецификациям верхнего уровня ;
- помимо описательных, должны быть представлены формальные спецификации верхнего уровня. Необходимо использовать современные методы формальной спецификации и верификации систем;
- механизм конфигурационного управления должен распространяться на весь жизненный цикл и все компоненты системы, имеющие отношение к обеспечению безопасности;
- должно быть описано соответствие между формальными спецификациями верхнего уровня и исходными текстами.

Классы коротко

- уровень C - произвольное управление доступом;
- уровень B - принудительное управление доступом;
- уровень A - верифицируемая безопасность.

Стандарт ISO/IEC 15408

"Критериев оценки безопасности информационных технологий" (издан 1 декабря 1999 года). Этот международный стандарт стал итогом почти десятилетней работы специалистов нескольких стран, он вобрал в себя опыт существовавших к тому времени документов национального и межнационального масштаба.

Данный стандарт часто называют "Общими критериями" (или даже ОК).

"Общие критерии" на самом деле являются метастандартом, определяющим инструменты оценки безопасности ИС и порядок их использования. В отличие от "Оранжевой книги", ОК не содержат предопределенных "классов безопасности". Такие классы можно строить, исходя из **требований безопасности**, существующих для конкретной организации и/или конкретной информационной системы.

Стандарт ISO/IEC 15408

ОК содержат два основных вида **требований** безопасности:

- **функциональные**, соответствующие активному аспекту защиты, предъявляемые к функциям безопасности и реализующим их механизмам;
- **требования доверия**, соответствующие пассивному аспекту, предъявляемые к технологии и процессу разработки и эксплуатации.

Требования безопасности предъявляются, а их выполнение проверяется для определенного **объекта оценки** - аппаратно-программного продукта или информационной системы.

Стандарт ISO/IEC 15408

Безопасность в ОК рассматривается не статично, а в привязке к жизненному циклу объекта оценки. Выделяются следующие этапы:

- определение назначения, условий применения, целей и требований безопасности;
- проектирование и разработка;
- испытания, оценка и сертификация;
- внедрение и эксплуатация.

Стандарт ISO/IEC 15408

В ОК объект оценки рассматривается в контексте **среды безопасности**, которая характеризуется определенными условиями и угрозами.

В свою очередь, угрозы характеризуются следующими параметрами:

- источник угрозы;
- метод воздействия;
- уязвимые места, которые могут быть использованы;
- ресурсы (активы), которые могут пострадать.

Уязвимые места могут возникать из-за недостатка:

- требований безопасности;
- проектирования;
- эксплуатации.

Стандарт ISO/IEC 15408

В "Общих критериях" введена иерархия **класс-семейство-компонент-элемент**.

- **Классы** определяют наиболее общую, "предметную" группировку требований (например, функциональные требования подотчетности).
- **Семейства** в пределах класса различаются по строгости и другим нюансам требований.
- **Компонент** - минимальный набор требований, фигурирующий как целое.
- **Элемент** - неделимое требование.

Стандарт ISO/IEC 15408

Профиль защиты (ПЗ) представляет собой типовой набор требований, которым должны удовлетворять продукты и/или системы определенного класса (например, операционные системы на компьютерах в правительственных организациях).

Задание по безопасности содержит совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности.

В ОК нет готовых классов защиты. Сформировать классификацию в терминах "Общих критериев" - значит определить несколько иерархически упорядоченных профилей защиты, в максимально возможной степени использующих стандартные функциональные требования и требования **доверия безопасности**.

Стандарт ISO/IEC 15408

- **Функциональный пакет** - это неоднократно используемая совокупность компонентов, объединенных для достижения определенных целей безопасности. "Общие критерии" не регламентируют структуру пакетов, процедуры верификации, регистрации и т.п., отводя им роль технологического средства формирования ПЗ.
- Базовый профиль защиты должен включать требования к основным (обязательным в любом случае) возможностям. Производные профили получаются из базового путем добавления необходимых пакетов расширения, то есть подобно тому, как создаются производные классы в объектно-ориентированных языках программирования.

Классы функциональных требований (11 классов, 66 семейств, 135 компонентов)

- идентификация и аутентификация ;
- **защита данных пользователя** ;
- **защита функций безопасности** (требования относятся к целостности и контролю данных сервисов безопасности и реализующих их механизмов);
- **управление безопасностью** (требования этого класса относятся к управлению атрибутами и параметрами безопасности);
- **аудит безопасности** (выявление, регистрация, хранение, анализ данных, затрагивающих безопасность объекта оценки, реагирование на возможное нарушение безопасности);
- **доступ к объекту оценки** ;
- **приватность** (защита пользователя от раскрытия и несанкционированного использования его идентификационных данных);
- **использование ресурсов** (требования к доступности информации);
- **криптографическая поддержка** (управление ключами);
- **связь** (аутентификация сторон, участвующих в обмене данными);
- **доверенный маршрут/канал** (для связи с сервисами безопасности).

Классы требований доверия (10 классов, 44 семейства, 93 компонента)

- разработка (требования для поэтапной детализации функций безопасности от краткой спецификации до реализации);
- поддержка жизненного цикла (включая порядок устранения недостатков и защиту среды разработки);
- тестирование ;
- **оценка уязвимостей** (включая оценку стойкости функций безопасности);
- **поставка и эксплуатация** ;
- управление конфигурацией;
- руководства (требования к эксплуатационной документации);
- **поддержка доверия** (для поддержки этапов жизненного цикла после сертификации);
- оценка профиля защиты;
- оценка задания по безопасности.

Оценочные уровни доверия

Применительно к требованиям доверия в "Общих критериях" сделана весьма полезная вещь, не реализованная, к сожалению, для функциональных требований. Введены **оценочные уровни доверия**, содержащие осмысленные комбинации компонентов.

- Оценочный уровень доверия 1 (начальный) предусматривает анализ **функциональной спецификации**, спецификации интерфейсов, эксплуатационной документации, а также независимое тестирование. Уровень применим, когда угрозы не рассматриваются как серьезные.
- Оценочный уровень доверия 2, в дополнение к первому уровню, предусматривает наличие **проекта верхнего уровня** объекта оценки, выборочное независимое тестирование, анализ стойкости функций безопасности, поиск разработчиком явных уязвимых мест.
- На третьем уровне ведется контроль среды разработки и управление конфигурацией объекта оценки.

Оценочные уровни доверия

- На уровне 4 добавляются полная спецификация интерфейсов, **проекты нижнего уровня**, анализ подмножества реализации, применение неформальной **модели** политики безопасности, независимый анализ уязвимых мест, автоматизация управления конфигурацией. Вероятно, это самый высокий уровень, которого можно достичь при существующей технологии программирования и приемлемых затратах.
- Уровень 5, в дополнение к предыдущим, предусматривает применение формальной модели политики безопасности, полуформальных функциональной спецификации и проекта верхнего уровня с **демонстрацией соответствия** между ними. Необходимо проведение анализа скрытых каналов разработчиками и оценщиками.
- На уровне 6 реализация должна быть представлена в структурированном виде. Анализ соответствия распространяется на проект нижнего уровня.
- Оценочный уровень 7 (самый высокий) предусматривает формальную верификацию проекта объекта оценки. Он применим к ситуациям чрезвычайно высокого риска.

Сетевая модель OSI

- Сетевая модель OSI (англ. open systems interconnection basic reference model — базовая эталонная модель взаимодействия открытых систем; 1978 г) — сетевая модель стека сетевых протоколов. Разработана Международной организацией по стандартам (International Standardization Organization - ISO)
- В связи с затянувшейся разработкой протоколов OSI, в настоящее время основным используемым стеком протоколов является TCP/IP, разработанный ещё до принятия модели OSI и вне связи с ней.
- Любой протокол модели OSI должен взаимодействовать либо с протоколами своего уровня, либо с протоколами на единицу выше и/или ниже своего уровня. Взаимодействия с протоколами своего уровня называются горизонтальными, а с уровнями на единицу выше или ниже — вертикальными. Любой протокол модели OSI может выполнять только функции своего уровня и не может выполнять функций другого уровня.

Сетевая модель OSI

Тип данных	Уровень (layer)	Функции
Данные	7. Прикладной (application)	Доступ к сетевым службам
	6. Представительский (presentation)	Представление и шифрование данных
	5. Сеансовый (session)	Управление сеансом связи
Сегменты	4. Транспортный (transport)	Прямая связь между конечными пунктами и надежность
Пакеты	3. Сетевой (network)	Определение маршрута и логическая адресация
Кадры	2. Канальный (data link)	Физическая адресация
Биты	1. Физический (physical)	Работа со средой передачи, сигналами и двоичными данными

Руководящие документы Гостехкомиссии России (ФСТЭК России)

5 января 1992 года была создана Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России).

В соответствии с Указом Президента Российской Федерации от 9 марта 2004 г. № 314 «О системе и структуре федеральных органов исполнительной власти» вместо существовавшей Государственной технической комиссии при Президенте Российской Федерации была создана Федеральная служба по техническому и экспортному контролю Российской Федерации.

Положение о Службе утверждено Указом Президента РФ от 16 августа 2004 г. № 1085.

С 20 мая 2005 года служба стала называться **Федеральная служба по техническому и экспортному контролю (ФСТЭК России)**.

Гостехкомиссия России в период своего существования вела весьма активную нормотворческую деятельность, выпуская Руководящие документы (РД), играющие роль национальных оценочных стандартов в области информационной безопасности.

Руководящие документы Гостехкомиссии России (ФСТЭК России)

1. Руководящий документ Гостехкомиссии России «**Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации**». – М.: ГТК РФ, 1992. – 39 с.
2. Руководящий документ Гостехкомиссии России «**Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники**». – М.: ГТК РФ, 1992. – 29 с.
3. Руководящий документ Гостехкомиссии России «**Защита от несанкционированного доступа к информации. Термины и определения**». – М.: ГТК РФ, 1992. – 13 с.
4. Руководящий документ Гостехкомиссии России «**Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации**». – М.: ГТК РФ, 1992. – 12 с.
5. Руководящий документ Гостехкомиссии России «**Средства вычислительной техники защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации**». – М.: ГТК РФ, 1992. – 24 с.
6. Руководящий документ Гостехкомиссии России «**Защита информации. Специальные защитные знаки. Классификация и общие требования**». – М.: ГТК РФ, 1997. – 7 с.
7. Руководящий документ Гостехкомиссии России «**Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации**». – М.: ГТК РФ, 1997. – 18 с.
8. Руководящий документ Гостехкомиссии России «**Защита информации в контрольно-кассовых машинах и автоматизированных кассовых системах. Классификация контрольно-кассовых машин, автоматизированных кассовых систем и требования по защите информации**» // Сборник руководящих документов по защите информации от несанкционированного доступа. – М.: ГТК РФ, 1998. – 11 с.
9. Руководящий документ Гостехкомиссии России «**Защита от несанкционированного доступа к информации**». – М.: ГТК РФ, 1999. – 11 с.

Руководящие документы Гостехкомиссии России (ФСТЭК России)

Рассмотрим Классификацию **автоматизированных систем (АС)** по уровню **защищенности от несанкционированного доступа (НСД)**.

Устанавливается 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 (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС.

Руководящие документы Гостехкомиссии России (ФСТЭК России)

Третья группа классифицирует АС, в которых работает один пользователь, имеющий доступ ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса - 3Б и 3А.

Вторая группа классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранящейся на носителях различного уровня конфиденциальности. Группа содержит два класса - 2Б и 2А.

Первая группа классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов - 1Д, 1Г, 1В, 1Б и 1А.

Таблица требований к девяти классам защищенности АС.

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
1. Подсистема управления доступом 1.1. Идентификация, проверка подлинности и контроль доступа субъектов: в систему;	+	+	+	+	+	+	+	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ;	-	-	-	+	-	+	+	+	+
к программам;	-	-	-	+	-	+	+	+	+
к томам, каталогам, файлам, записям, полям записей.	-	-	-	+	-	+	+	+	+
1.2. Управление потоками информации	-	-	-	+	-	-	+	+	+
2. Подсистема регистрации и учета 2.1. Регистрация и учет: входа/выхода субъектов доступа в/из системы (узла сети);	+	+	+	+	+	+	+	+	+
выдачи печатных (графических) выходных документов;	-	+	-	+	-	+	+	+	+
запуска/завершения программ и процессов (заданий, задач);	-	-	-	+	-	+	+	+	+

"-" нет требований к данному классу; "+" есть требования к данному классу;

Таблица требований к девяти классам защищенности АС (продолжение).

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей;	-	-	-	+	-	+	+	+	+
изменения полномочий субъектов доступа;	-	-	-	-	-	-	+	+	+
создаваемых защищаемых объектов доступа.	-	-	-	+	-	-	+	+	+
2.2. Учет носителей информации.	+	+	+	+	+	+	+	+	+
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей.	-	+	-	+	-	+	+	+	+
2.4. Сигнализация попыток нарушения защиты.	-	-	-	-	-	-	+	+	+
3. Криптографическая подсистема 3.1. Шифрование конфиденциальной информации.	-	-	-	+	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах.	-	-	-	-	-	-	-	-	+

"-" нет требований к данному классу; "+" есть требования к данному классу;

Таблица требований к девяти классам защищенности АС (продолжение).

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+
4. Подсистема обеспечения целостности 4.1. Обеспечение целостности программных средств и обрабатываемой информации.	+	+	+	+	+	+	+	+	+
4.2. Физическая охрана средств вычислительной техники и носителей информации.	+	+	+	+	+	+	+	+	+
4.3. Наличие администратора (службы защиты) информации в АС.	-	-	-	+	-	-	+	+	+
4.4. Периодическое тестирование СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.5. Наличие средств восстановления СЗИ НСД.	+	+	+	+	+	+	+	+	+
4.6. Использование сертифицированных средств защиты.	-	+	-	+	-	-	+	+	+
3.3. Использование аттестованных (сертифицированных) криптографических средств.	-	-	-	+	-	-	-	+	+

"-" нет требований к данному классу; "+" есть требования к данному классу;

Руководящие документы Гостехкомиссии России (ФСТЭК России)

"СЗИ НСД" система защиты информации от несанкционированного доступа

По существу перед нами - минимум требований, которым необходимо следовать, чтобы обеспечить конфиденциальность информации. Целостность представлена отдельной подсистемой (номер 4), но непосредственно к интересующему нас предмету имеет отношение только пункт 4.1. Доступность (точнее, восстановление) предусмотрено только для самих средств защиты.