Теоретические основы компьютерной безопасности

Лекция №10. Критерии и классы защищенности компьютерных систем

Учебные вопросы:

1. Нормативные документы по технической защите компьютерной информации .

Литература:

1. Сборник руководящих документов по защите информации от несанкционированного доступа. Гостехкомиссия при Президенте РФ. М: 1998 г.

2. Основы организационного обеспечения информационной безопасности объектов информатизации. С.Н. Семкин, Э.В. Беляков, С.В. Гребенев, В.И. Козачек. М.: «Гелиос АРВ», 2005.

3. Информационная безопасность. А.В. Бабаш, Е.К. Баранова, Ю. Н. Мельников. Учебное пособие: 2012.

Вопрос №1. Нормативные документы по технической защите компьютерной информации

Нормативные документы Гостехкомиссии при Президенте РФ (ФСТЭК)

- **РД. Средства вычислительной техники, защита от НСД к информации. Показатели защищенности от НСД**
- **РД. Автоматизированные системы защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации.**
- **РД. Средства вычислительной техники. Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации**
- **Положение по аттестации объектов информатизации по требованиям безопасности информации**

РД СВТ. Защита от НСД к информации. Показатели защищенности от НСД

Разработан: Гостехкомиссией при Президенте РФ в 1992 г. на основе стандарта Минобороны США «Критерии оценки компьютерных систем» (Оранжевая книга).

Назначение РД: устанавливает классификацию средств вычислительной техники по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищенности и совокупности описывающих их требований.

Разделы РД:

1. Общие положения;
2. Требования к показателям защищенности.

Общие положения

1. Устанавливается **семь классов защищенности СВТ от НСД** к информации. Самый низкий класс – седьмой, самый высокий – первый;

2. Классы подразделяются на четыре группы, отличающиеся качественным уровнем защиты:

- первая группа содержит только один седьмой класс;
- вторая группа характеризуется дискреционной защитой и содержит шестой и пятый классы;
- третья группа характеризуется мандатной защитой и содержит четвертый, третий и второй классы;
- четвертая группа характеризуется верифицированной защитой и содержит только первый класс;

3. Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса.

Требования к показателям защищенности

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
1. Дискреционный принцип контроля доступа	+	+	+	=	+	=
2. Мандатный принцип контроля доступа	-	-	+	=	=	=
3. Очистка памяти	-	+	+	+	=	=
4. Изоляция модулей	-	-	+	=	+	=
5. Маркировка документов	-	-	+	=	=	=
6. Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
7. Сопоставление пользователя с устройством	-	-	+	=	=	=
8. Идентификация и аутентификация	+	=	+	=	=	=
9. Гарантия проектирования	-	+	+	+	+	+
10. Регистрация	-	+	+	+	=	=
11. Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
12. Надежное восстановление	-	-	-	+	=	=
13. Целостность КСЗ	-	+	+	+	=	=
14. Контроль модификации	-	-	-	-	+	=
15. Контроль дистрибуции	-	-	-	-	+	=
16. Гарантии архитектуры	-	-	-	-	-	+
17. Тестирование	+	+	+	+	+	=
18. Руководство пользователя	+	=	=	=	=	=
19. Руководство по КСЗ	+	+	=	+	+	=
20. Текстовая документация	+	+	+	+	+	=
21. Конструкторская (проектная) документация	+	+	+	+	+	+

Требования к показателям защищенности шестого класса

I. Дискретный принцип контроля доступа

1. Комплекс средств защиты (КСЗ) должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.);
2. КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа;
3. Контроль доступа должен быть применим к каждому объекту и каждому субъекту;
4. Механизм, реализующий дискретный принцип контроля доступа, должен предусматривать возможности санкционированного изменения правила разграничения доступа, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов;
5. Права изменять правила разграничения доступа должны предоставляться выделенным субъектам (администрации, службе безопасности).

II. Идентификация и аутентификация

1. Комплекс средств защиты должен требовать от пользователей идентифицировать себя при запросах на доступ;

2. КСЗ должен подвергать проверке подлинность идентификации – осуществлять аутентификацию;

3. КСЗ должен располагать необходимыми данными для идентификации и аутентификации;

4. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

III. Тестирование

В СВТ шестого класса должны тестироваться:

- реализация дискреционных правил разграничения доступа (перехват явных и скрытых запросов, правильное распознавание санкционированных и несанкционированных запросов на доступ, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);

- успешное осуществление идентификации и аутентификации, а также их средств защиты.

IV. Руководство для пользователя

Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования комплекса средств защиты и его интерфейса с пользователем.

V. Руководство по комплексу средств защиты

Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации комплекса средств защиты;
- описание старта СВТ и процедур проверки правильности старта.

VI. Тестовая документация

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ и результатов тестирования.

VII. Конструкторская (проектная) документация

Должна содержать общее описание принципов работы СВТ, общую схему комплекса средств защиты, описание интерфейсов комплекса средств защиты с пользователем и интерфейсов частей комплекса средств защиты между собой, описание механизмов идентификации и аутентификации.

РД. Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации

Разработан: Гостехкомиссией при Президенте РФ в 1992 г.

Назначение РД: устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в автоматизированных системах различных классов. Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков автоматизированных систем при формировании и реализации требований по защите.

Разделы РД:

1. Классификация автоматизированных систем;
2. Требования по защите информации от НСД для АС.

Классификация автоматизированных систем

1. Устанавливается **девять классов** защищенности АС от НСД к информации;

2. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС;

3. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности АС;

4. Третья группа классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – **3Б** и **3А**;

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

6. 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**.

Требования по защите информации от НСД для 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 терминам, 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)	+	+	+	+	+	+	+	+	+
Выдача печатных (графических) выходных документов		+		+		+	+	+	+

Подсистемы и требования	Классы								
	3Б	3А	2Б	2А	1Д	1Г	1В	1Б	1А
Запуска/завершения программ и процессов (заданий, задач)				+		+	+	+	+
Доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, 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 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									+

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		+		+			+	+	+

Требования к классу защищенности 3Б

I. Подсистема управления доступом

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов.

II. Подсистема регистрации и учета

1. Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС;
2. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

III. Подсистема обеспечения целостности

1. Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды;

2. При этом:

- целостность СЗИ НСД проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗИ;

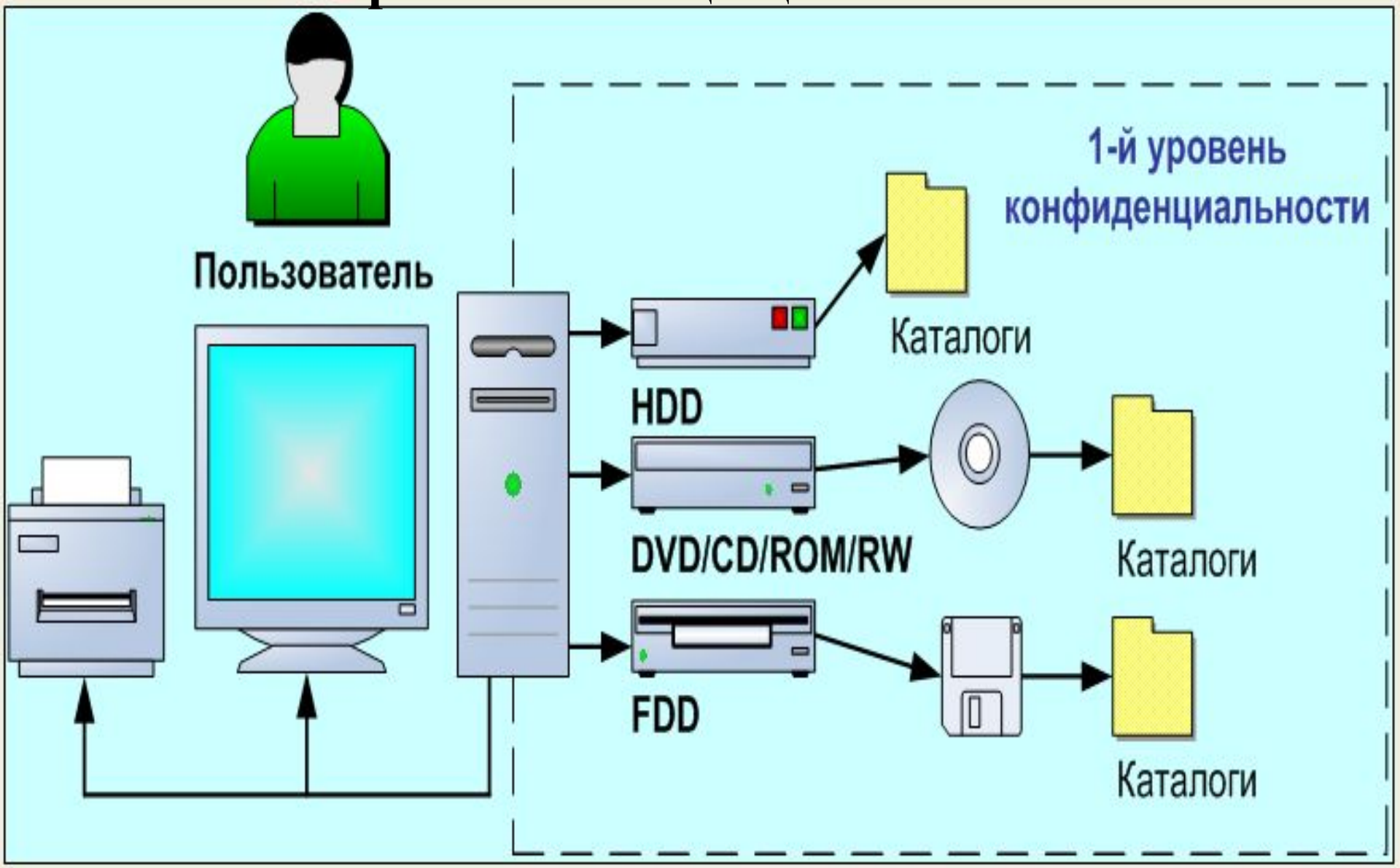
- целостность программной среды обеспечивается отсутствием в АС средств разработки и отладки программ;

- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

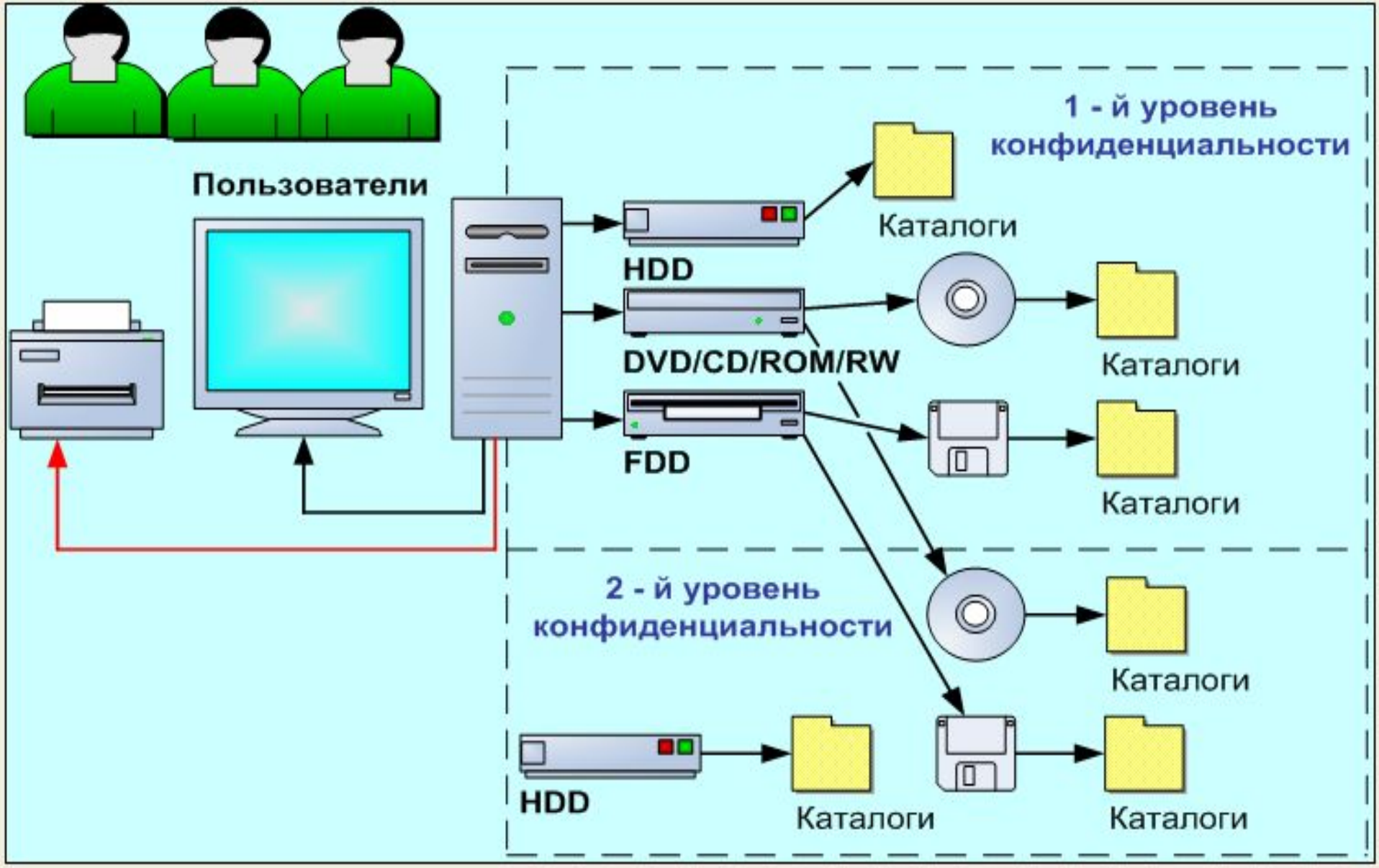
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;

- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

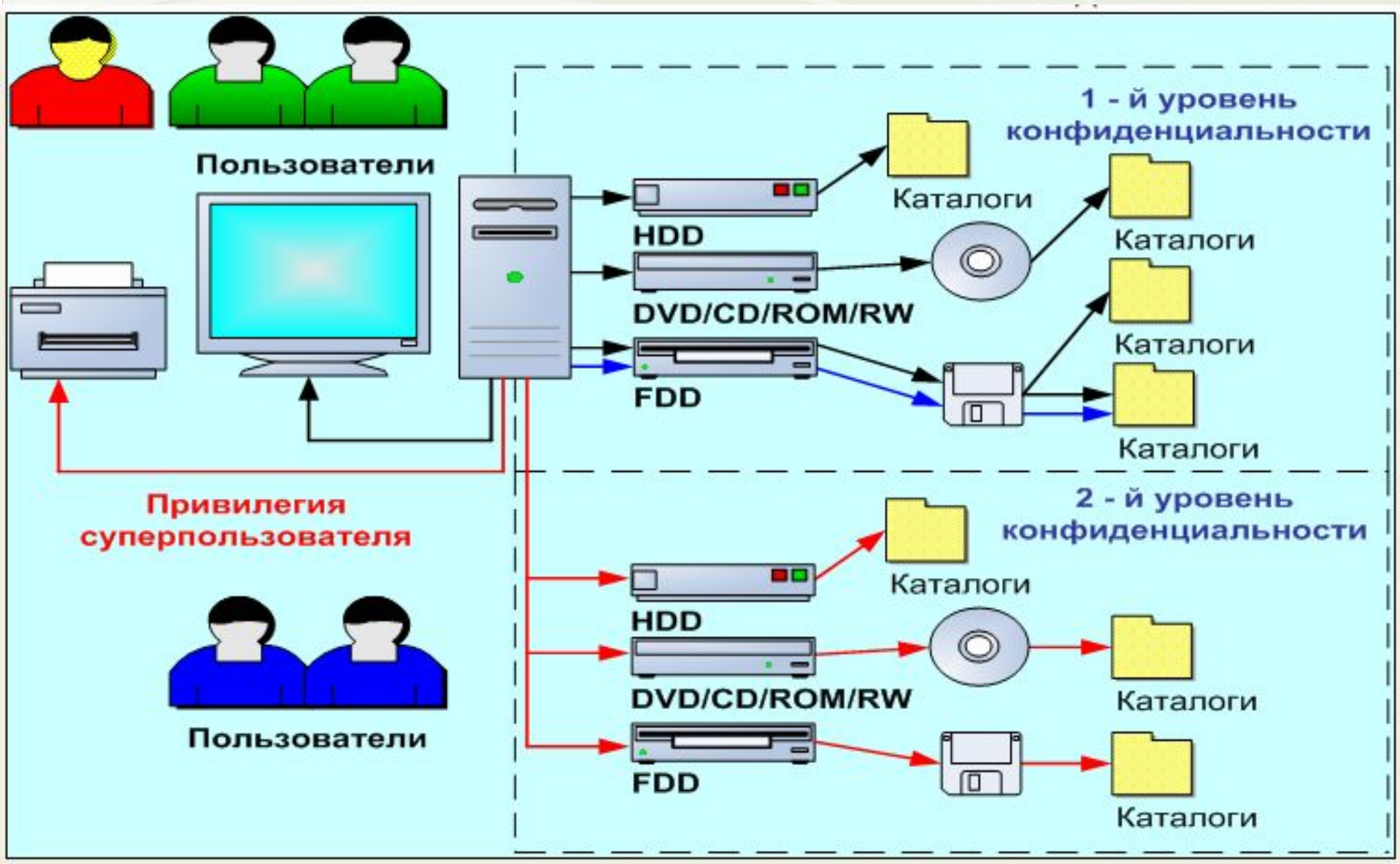
Вариант организации доступа к ресурсам АС при классе защищенности 3Б

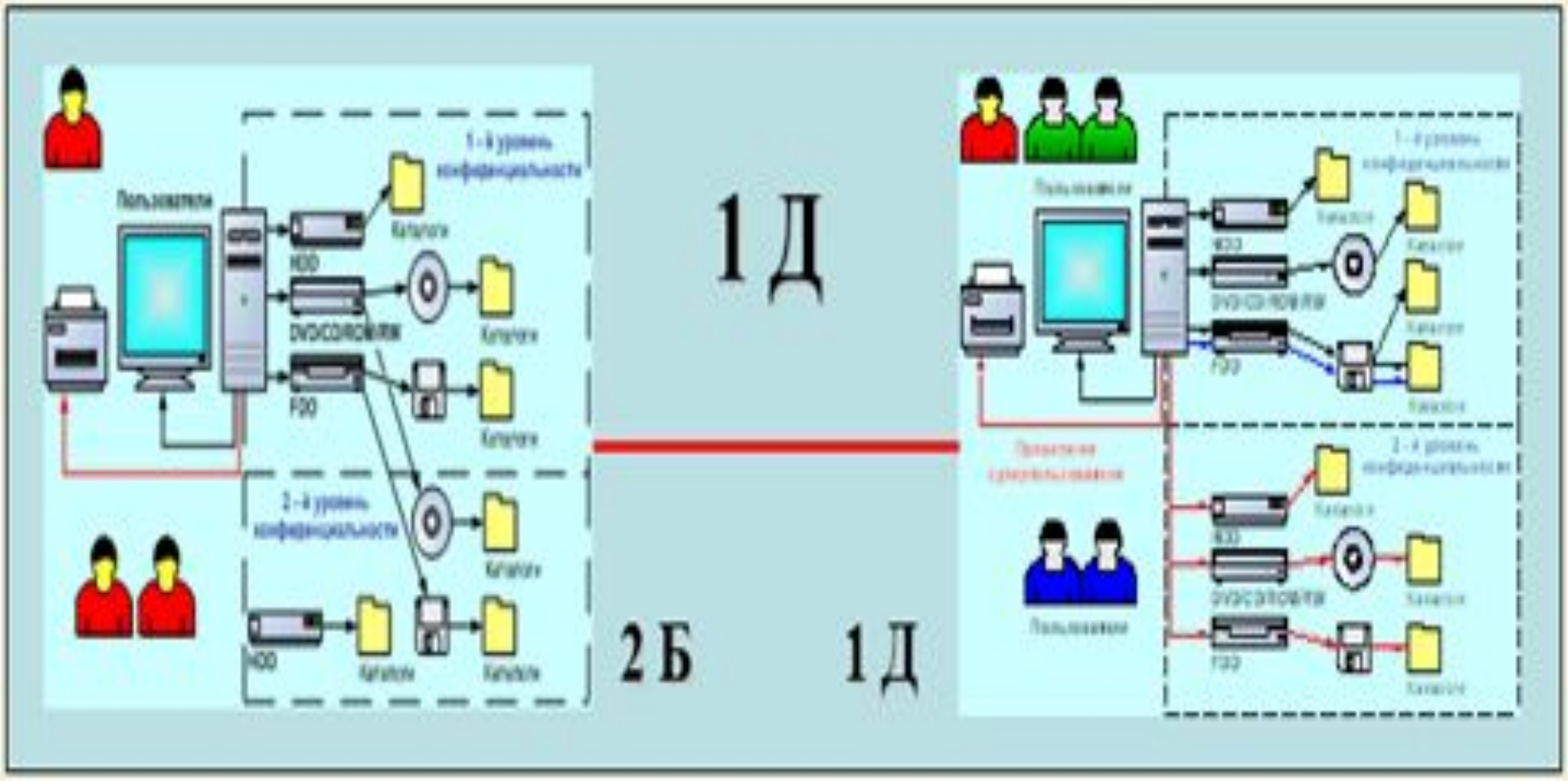


Вариант организации доступа к ресурсам АС при классе защищенности 2Б



Вариант организации доступа к ресурсам АС при классе защищенности 1 Г, Д




1 Д
2 Б
1 Д

РД . Межсетевые экраны. Защита от НСД к информации. Показатели защищенности от НСД к информации

Разработан: Гостехкомиссией при Президенте РФ в 1997 г.

Назначение РД: устанавливает классификацию межсетевых экранов (МЭ) по уровню защищенности от несанкционированного доступа (НСД) к информации на базе перечня показателей защищенности и совокупности описывающих их требований. Документ предназначен для заказчиков и разработчиков МЭ, а также сетей ЭВМ, распределенных автоматизированных систем с целью использования при формулировании и реализации требований по их защите от НСД к информации.

Разделы РД:

1. Общие положения;
2. Требования к межсетевым экранам.

Общие положения

1. Под Межсетевой экран (МЭ) подразумевают – локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС;

2. Устанавливается пять классов защищенности МЭ. Каждый класс характеризуется определенной минимальной совокупностью требований по защите информации. Самый низкий класс защищенности - пятый, применяемый для безопасного взаимодействия АС класса 1Д с внешней средой, четвертый - для 1Г, третий - 1В, второй - 1Б, самый высокий - первый, применяемый для безопасного взаимодействия АС класса 1А с внешней средой;

3. При включении МЭ в АС определенного класса защищенности, класс защищенности совокупной АС, полученной из исходной путем добавления в нее МЭ, не должен понижаться.

Для АС класса 3Б, 2Б должны применяться МЭ не ниже 5 класса.

Для АС класса 3А, 2А в зависимости от важности обрабатываемой информации должны применяться МЭ следующих классов:

- при обработке информации с грифом «секретно» - не ниже 3 класса;
- при обработке информации с грифом «совершенно секретно» - не ниже 2 класса;
- при обработке информации с грифом «особой важности» - не ниже 1 класса.

Требования к межсетевым экранам

Показатели защищенности	Классы защищенности				
	5	4	3	2	1
Управление доступом (фильтрация данных и трансляция адресов)	+	+	+	+	=
Идентификация и аутентификация	-	-	+	=	+
Регистрация	-	+	+	+	=
Администрирование: идентификация и аутентификация	+	=	+	+	+
Администрирование: регистрация	+	+	+	=	=
Администрирование: простота использования	-	-	+	=	+
Целостность	+	=	+	+	+
Восстановление	+	=	=	+	+
Тестирование	+	+	+	+	+
Руководство администратора защиты	+	=	=	=	=
Тестовая документация	+	+	+	+	+
Конструкторская (проектная) документация	+	=	+	=	+

Требования к пятому классу защищенности МЭ

I. Управление доступом

МЭ должен обеспечивать фильтрацию на сетевом уровне.

Решение по фильтрации может приниматься для каждого сетевого пакета независимо на основе, по крайней мере, сетевых адресов отправителя и получателя или на основе других эквивалентных атрибутов.

II. Администрирование: идентификация и аутентификация

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его локальных запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю условно-постоянного действия.

III. Администрирование: регистрация

1. МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова;

2. В параметрах регистрации указываются:

- дата, время и код регистрируемого события;
- результат попытки осуществления регистрируемого события - успешная или неуспешная;
- идентификатор администратора МЭ, предъявленный при попытке осуществления регистрируемого события.

IV. Целостность

МЭ должен содержать средства контроля за целостностью своей программной и информационной части.

V. Восстановление

МЭ должен предусматривать процедуру восстановления после сбоев и отказов оборудования, которые должны обеспечивать восстановление свойств МЭ.

VI. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:

- реализации правил фильтрации;
- процесса идентификации и аутентификации администратора МЭ;
- процесса регистрации действий администратора МЭ;
- процесса контроля за целостностью программной и информационной части МЭ;
- процедуры восстановления.

VII. Руководство администратора МЭ

Документ содержит:

- описание контролируемых функций МЭ;
- руководство по настройке и конфигурированию МЭ;
- описание старта МЭ и процедур проверки правильности старта;
- руководство по процедуре восстановления.

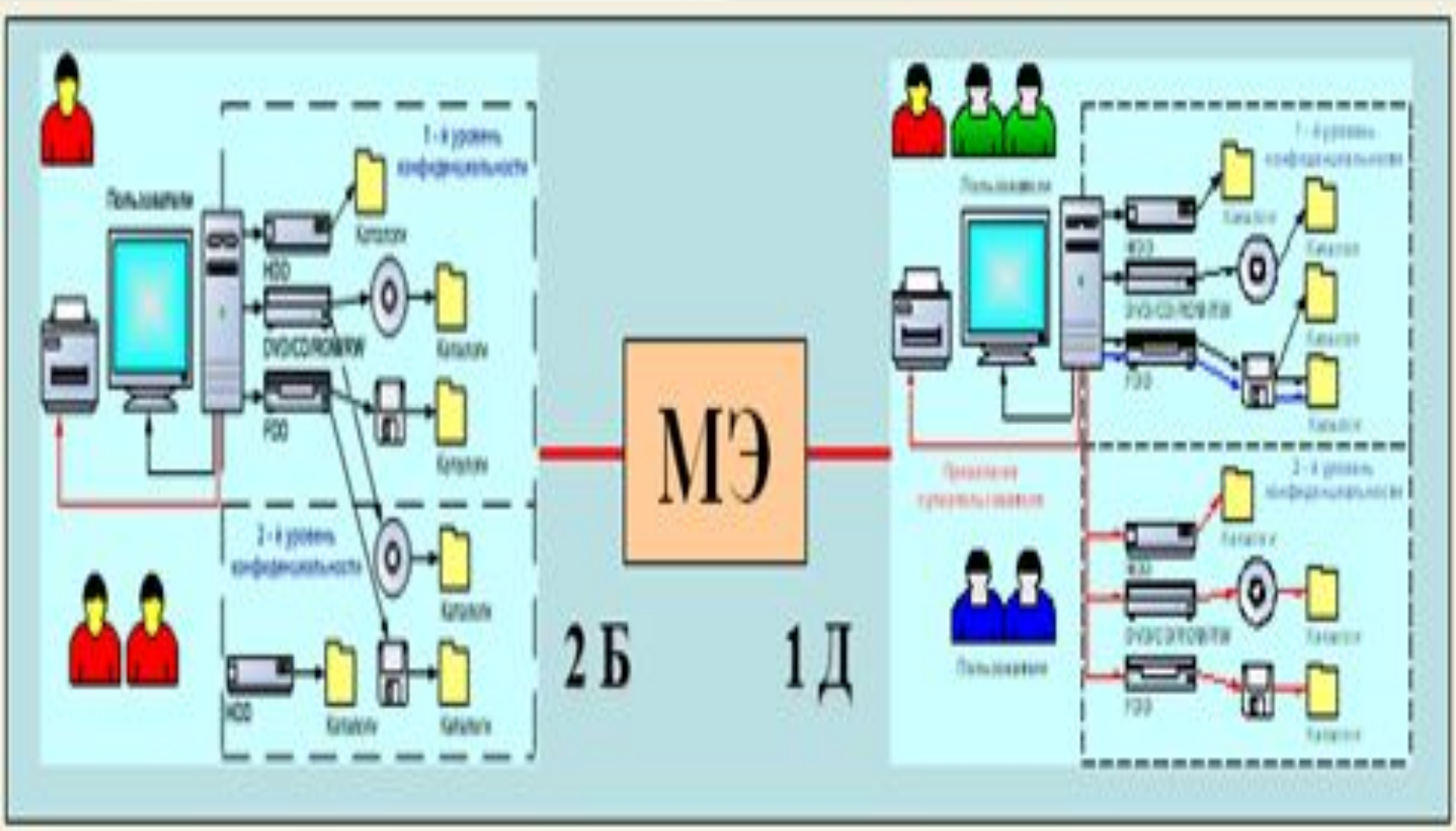
VIII. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ, и результаты тестирования.

IX. Конструкторская (проектная) документация

Должна содержать:

- общую схему МЭ;
- общее описание принципов работы МЭ;
- описание правил фильтрации;
- описание средств и процесса идентификации и аутентификации;
- описание средств и процесса регистрации;
- описание средств и процесса контроля за целостностью программной и информационной части МЭ;
- описание процедуры восстановления свойств МЭ.


МЭ
2 Б
1 Д

Положение по аттестации объектов информатизации по требованиям безопасности информации

Разработано: Гостехкомиссией при Президенте РФ в 1994 г.

Назначение: устанавливает основные принципы, организационную структуру системы аттестации объектов информатизации по требованиям безопасности информации, порядок проведения аттестации, а также контроля и надзора за аттестацией и эксплуатацией аттестованных объектов информатизации.

Разделы РД:

1. Общие положения;
2. Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации.
3. Порядок проведения аттестации.
4. Требования к нормативным и методическим документам по аттестации объектов информатизации.

Общие положения

1. Под аттестацией объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – «Аттестата соответствия» подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утвержденных Гостехкомиссией России;

2. Обязательной аттестации подлежат объекты информатизации, предназначенные для обработки информации, составляющей государственную тайну, управления экологически опасными объектами, ведения секретных переговоров;

В остальных случаях аттестация носит добровольный характер (добровольная аттестация) и может осуществляться по инициативе заказчика или владельца объекта информатизации;

3. При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счет побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на нее за счет специальных устройств, встроенных в объекты информатизации;

4. Аттестация предусматривает комплексную проверку (аттестационные испытания) защищаемого объекта информатизации в реальных условиях эксплуатации с целью оценки соответствия применяемого комплекса мер и средств защиты требуемому уровню безопасности информации;

5. Проводимые работы при Аттестация:

- анализ исходных данных по аттестуемому объекту информатизации;
- предварительное ознакомление с аттестуемым объектом информатизации;
- проведение экспертного обследования объекта информатизации и анализ разработанной документации по защите информации на этом объекте;
- проведение испытаний отдельных средств и систем защиты информации на аттестуемом объекте информатизации с помощью специальной контрольной аппаратуры и тестовых средств;
- проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- проведение комплексных аттестационных испытаний объекта информатизации в реальных условиях эксплуатации;
- анализ результатов экспертного обследования и комплексных аттестационных испытаний объекта информатизации и утверждение заключения по результатам аттестации.

Организационная структура системы аттестации объектов информатизации по требованиям безопасности информации

1. Федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации – Гостехкомиссия России (ФСТЭК)

2. Органы по аттестации объектов информатизации по требованиям безопасности информации

3. Испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации

4. Заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации)

Порядок проведения аттестации и контроля

Порядок проведения аттестации объектов информатизации по требованиям безопасности информации включает следующие действия:

- подачу и рассмотрение заявки на аттестацию;
- предварительное ознакомление с аттестуемым объектом;
- испытание несертифицированных средств и систем защиты информации, используемых на аттестуемом объекте (при необходимости);
- разработка программы и методики аттестационных испытаний;
- заключение договоров на аттестацию;
- проведение аттестационных испытаний объекта информатизации;
- оформление, регистрация и выдача «Аттестата соответствия»;
- осуществление государственного контроля и надзора, инспекционного контроля за проведением аттестации и эксплуатацией аттестованных объектов информатизации;
- рассмотрение апелляций.

Требования к нормативным и методическим документам по аттестации объектов информатизации

1. Объекты информатизации, вне зависимости от используемых отечественных или зарубежных технических и программных средств, аттестуются на соответствие требованиям государственных стандартов или иных нормативных документов по безопасности информации, утвержденных Гостехкомиссией России;

2. Состав нормативной и методической документации для аттестации конкретных объектов информатизации определяется органом по аттестации в зависимости от вида и условий функционирования объектов информатизации на основании анализа исходных данных по аттестуемому объекту;

3. В нормативную документацию включаются только те показатели, характеристики, требования, которые могут быть объективно проверены;

4. В нормативной и методической документации на методы испытаний должны быть ссылки на условия, содержание и порядок проведения испытаний, используемые при испытаниях контрольную аппаратуру и тестовые средства, сводящие к минимуму погрешности результатов испытаний и позволяющие воспроизвести эти результаты;

5. Тексты нормативных и методических документов, используемых при аттестации объектов информатизации, должны быть сформулированы ясно и четко, обеспечивая их точное и единообразное толкование.