Комплексная защита информации конфиденциального характера

Тема . Руководящие документы по защите конфиденциальной информации

Руководящие документы ФСТЭК

1. «Автоматизированные системы.
   Защита от несанкционированного доступа к информации.
   Классификация АС и требования по защите информации».
2. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».
3. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».
4. «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

1. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация АС и требования по защите информации».

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Принятые сокращения

АС - автоматизированные системы

НСД - несанкционированный доступ

РД - руководящий документ

СЗИ - система защиты информации

СЗИ НСД - система защиты информации от несанкционированного доступа

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Классификация АС

Классификация распространяется на все действующие и проектируемые АС учреждений, организаций и предприятий, обрабатывающие конфиденциальную информацию.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Основными этапами классификации АС являются:

- разработка и анализ исходных данных;
- выявление основных признаков АС, необходимых для классификации;
- сравнение выявленных признаков АС с классифицируемыми;
- присвоение АС соответствующего класса защиты информации от НСД.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Необходимыми исходными данными для проведения классификации конкретной АС являются:

- перечень защищаемых информационных ресурсов АС и их уровень конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к защищаемым информационным ресурсам АС;
- режим обработки данных в АС.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Требования по защите информации от НСД для АС

В общем случае, комплекс программно-технических средств и организационных (процедурных) решений по защите информации от НСД реализуется в рамках системы защиты информации от НСД (СЗИ НСД), условно состоящей из следующих четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Требования к АС третьей группы

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

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Подсистемы и требования	Классы	
	3Б	3А
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	-	-

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме управления доступом для классов 3Б и 3А:

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

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

Подсистемы и требования	Классы	
	3Б	3А
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему(ы) (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	-
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	-
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	-	-

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме регистрации и учета для классов 3Б и 3А:

- 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. В параметрах регистрации указываются:

для класса 3 Б

- дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

для класса 3 А

- дополнительно указывается результат попытки входа: успешная или неуспешная (при НСД);

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Также в подсистеме регистрации и учета для классов 3Б и 3А:

- должен проводиться учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку).

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Для класса 3А дополнительно:

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
  - дата и время выдачи (обращения к подсистеме вывода);
  - краткое содержание документа (наименование, вид, код, шифр) и уровень его конфиденциальности
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
- должно проводиться несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Подсистемы и требования	Классы	
	3Б	3А
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	-
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Подсистемы и требования	Классы	
	3Б	3А
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	-	+

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме обеспечения целостности для классов 3Б и 3А:

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

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Также в подсистеме обеспечения целостности для классов 3Б и 3А:

- 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.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме обеспечения целостности для класса 3Б дополнительно:

- 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;

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме обеспечения целостности для класса 3А дополнительно:

- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;

- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Требования к АС второй группы

Вторая группа включает 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**.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Подсистемы и требования	Классы	
	2Б	2А
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	-	+

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме управления доступом для классов 2Б и 2А:

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

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме управления доступом для класса 2А дополнительно:

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по их логическим адресам (номерам);
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на них информации.

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

Подсистемы и требования	Классы	
	2Б	2А
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+
выдачи печатных (графических) выходных документов	-	+
запуска (завершения) программ и процессов (заданий, задач)	-	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+
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	-	-

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

В подсистеме регистрации и учета для класса 2Б

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная (при НСД);
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).

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

В подсистеме регистрации и учета для класса 2А

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная (при НСД);
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа порядковым номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
  - дата и время выдачи (обращения к подсистеме вывода);
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства], краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
  - идентификатор субъекта доступа, запросившего документ;
- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
  - дата и время запуска;
  - имя (идентификатор) программы (процесса, задания);
  - идентификатор субъекта доступа, запросившего программу (процесс, задание);
  - результат запуска (успешный, неуспешный - несанкционированный);

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

В подсистеме регистрации и учета для класса 2А

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого файла;
- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого объекта [логическое имя (номер)];

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

В подсистеме регистрации и учета для класса 2А

- должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

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

Подсистемы и требования	Классы	
	2Б	2А
3. Криптографическая подсистема		
3.1. Шифрование конфиденциальной информации	-	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	+

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

В криптографической подсистеме для класса 2А:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должны выполняться автоматическое освобождение и очистка областей внешней памяти, содержавших ранее незашифрованную информацию;

- доступ субъектов к операциям шифрования и криптографическим ключам должен дополнительно контролироваться подсистемой управления доступом;

- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

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

Подсистемы и требования	Классы	
	2Б	2А
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	-	+

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

В подсистеме обеспечения целостности для класса 2Б:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. 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 во время обработки и (или) хранения защищаемой информации;
- 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.

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

В подсистеме обеспечения целостности для класса 2А:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. 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;
- должны осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД;
- 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;
- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Требования к АС первой группы

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

РД. АС. Защита от НСД к информации. Классификация автоматизированных систем и требования по защите информации

Подсистемы и требования	Классы				
	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	-	-	+	+	+

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

В подсистема управления доступом для класса 1Д:

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

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

В подсистема управления доступом для класса 1Г:

- должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

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

В подсистема управления доступом для класса 1В:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам и (или) адресам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

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

В подсистема управления доступом для класса 1Б:

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов;
- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам);
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

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

В подсистема управления доступом для класса 1А

- должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов.
- должна осуществляться аппаратурная идентификация и проверка подлинности терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по уникальным встроенным устройствам;
- должна осуществляться идентификация и проверка подлинности программ, томов, каталогов, файлов, записей, полей записей по именам и контрольным суммам (паролям, ключам);
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа;
- должно осуществляться управление потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности записываемой на него информации.

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

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
2. Подсистема регистрации и учета					
2.1. Регистрация и учет:					
входа (выхода) субъектов доступа в (из) систему (узел сети)	+	+	+	+	+
выдачи печатных (графических) выходных документов	-	+	+	+	+
запуска (завершения) программ и процессов (заданий, задач)	-	+	+	+	+
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	-	+	+	+	+
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	-	-	+	+	+

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

В подсистеме регистрации и учета для класса 1Д

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная - несанкционированная;
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

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

В подсистеме регистрации и учета для класса 1Г

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная - несанкционированная;
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
  - код или пароль, предъявленный при неуспешной попытке;

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

В подсистеме регистрации и учета для класса 1Г

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:
  - дата и время выдачи (обращения к подсистеме вывода);
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
  - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
  - идентификатор субъекта доступа, запросившего документ;

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

В подсистеме регистрации и учета для класса 1Г

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
  - дата и время запуска;
  - имя (идентификатор) программы (процесса, задания);
  - идентификатор субъекта доступа, запросившего программу (процесс, задание);
  - результат запуска (успешный, неуспешный - несанкционированный);

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

В подсистеме регистрации и учета для класса 1Г

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого файла;

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

В подсистеме регистрации и учета для класса 1Г

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого объекта [логическое имя (номер)];

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

В подсистеме регистрации и учета для класса 1Г

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов);

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

В подсистеме регистрации и учета для класса 1В

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная - несанкционированная;
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
  - код или пароль, предъявленный при неуспешной попытке;

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). В параметрах регистрации указываются:
  - дата и время выдачи (обращение к подсистеме вывода);
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
  - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
  - идентификатор субъекта доступа, запросившего документ;
  - объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
  - дата и время запуска;
  - имя (идентификатор) программы (процесса, задания);
  - идентификатор субъекта доступа, запросившего программу (процесс, задание);
  - результат запуска (успешный, неуспешный - несанкционированный);

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому файлу с указанием ее результата:
    - успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого файла;
  - имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
  - вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого объекта [логическое имя (номер)];
  - имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
  - вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
  - дата и время изменения полномочий;
  - идентификатор субъекта доступа (администратора), осуществившего изменения;
- должен осуществляться автоматический учет создаваемых защищаемых файлов с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

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

В подсистеме регистрации и учета для класса 1В

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;

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

В подсистеме регистрации и учета для класса 1В

- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
- должна осуществляться сигнализация попыток нарушения защиты.

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

В подсистеме регистрации и учета для класса 1Б

- 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. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешный или неуспешный - несанкционированный;
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
  - код или пароль, предъявленный при неуспешной попытке;

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

В подсистеме регистрации и учета для класса 1Б

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:
  - дата и время выдачи (обращения к подсистеме вывода);
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
  - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
  - идентификатор субъекта доступа, запросившего документ;
  - объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный;

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

В подсистеме регистрации и учета для класса 1Б

- должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:
  - дата и время запуска;
  - имя (идентификатор) программы (процесса, задания);
  - идентификатор субъекта доступа, запросившего программу (процесс, задание);
  - результат запуска (успешный, неуспешный - несанкционированный);
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого файла;
  - имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
  - вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

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

В подсистеме регистрации и учета для класса 1Б

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого объекта [логическое имя (номер)];
  - имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
  - вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

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

В подсистеме регистрации и учета для класса 1Б

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
  - дата и время изменения полномочий;
  - идентификатор субъекта доступа (администратора), осуществившего изменения;
  - идентификатор субъекта, у которого проведено изменение полномочий и вид изменения (пароль, код, профиль и т.п.);
  - спецификация объекта, у которого проведено изменение статуса защиты и вид изменения (код защиты, уровень конфиденциальности);
- должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

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

В подсистеме регистрации и учета для класса 1Б

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки;
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, использованную для хранения защищаемой информации;
- должна осуществляться сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

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

В подсистеме регистрации и учета для класса 1А

- 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 останов не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:
  - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
  - результат попытки входа: успешная или неуспешная – несанкционированная;
  - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
  - код или пароль, предъявленный при неуспешной попытке;

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

В подсистеме регистрации и учета для класса 1А

- должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером и учетными реквизитами АС с указанием на последнем листе документа общего количества листов (страниц). Вместе с выдачей документа должна автоматически оформляться учетная карточка документа с указанием даты выдачи документа, учетных реквизитов документа, краткого содержания (наименования, вида, шифра, кода) и уровня конфиденциальности документа, фамилии лица, выдавшего документ, количества страниц и копий документа (при неполной выдаче документа - фактически выданного количества листов в графе «Брак»). В параметрах регистрации указываются:
  - дата и время выдачи (обращения к подсистеме вывода);
  - спецификация устройства выдачи [логическое имя (номер) внешнего устройства];
  - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа;
  - идентификатор субъекта доступа, запросившего документ;
  - объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи: успешный (весь объем), неуспешный;

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

В подсистеме регистрации и учета для класса 1А

- должна осуществляться регистрация запуска (завершения) всех программ и процессов (заданий, задач) в АС. В параметрах регистрации указываются:
  - дата и время запуска;
  - имя (идентификатор) программы (процесса, задания);
  - идентификатор субъекта доступа, запросившего программу (процесс, задание);
  - результат запуска (успешный, неуспешный - несанкционированный);
  - полная спецификация соответствующего файла "образа" программы (процесса, задания) - устройство (том, каталог), имя файла (расширение);
- должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная – несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого файла;
  - имя программы (процесса, задания, задачи), осуществляющей доступ к файлу, вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т.п.);

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

В подсистеме регистрации и учета для класса 1А

- должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются:
  - дата и время попытки доступа к защищаемому объекту с указанием ее результата: спешная, неуспешная - несанкционированная;
  - идентификатор субъекта доступа;
  - спецификация защищаемого объекта [логическое имя (номер)];
  - имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
  - вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.);

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

В подсистеме регистрации и учета для класса 1А

- должна осуществляться регистрация изменений полномочий субъектов доступа и статуса объектов доступа. В параметрах регистрации указываются:
  - дата и время изменения полномочий и статуса;
  - идентификатор субъекта доступа (администратора), осуществившего изменения;
  - идентификатор субъекта доступа, у которого изменены полномочия и вид изменений (пароль, код, профиль и т.п.);
  - спецификация объекта, у которого изменен статус защиты, и вид изменения (код защиты, уровень конфиденциальности);
- должен осуществляться автоматический учет создаваемых защищаемых файлов, инициируемых защищаемых томов, каталогов, областей оперативной памяти ЭВМ, выделяемых для обработки защищаемых файлов, внешних устройств ЭВМ, каналов связи, ЭВМ, узлов сети ЭВМ, фрагментов сети с помощью их дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта;

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

В подсистеме регистрации и учета для класса 1А

- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должно проводиться несколько видов учета (дублирующих) защищаемых носителей информации;
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, в которой содержалась защищаемая информация;
- должна осуществляться надежная сигнализация попыток нарушения защиты на терминал администратора и нарушителя.

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

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
3. Криптографическая подсистема					
3.1. Шифрование конфиденциальной информации	-	-	-	+	+
3.2. Шифрование информации, принадлежащей различным субъектам доступа (группам субъектов) на разных ключах	-	-	-	-	+
3.3. Использование аттестованных (сертифицированных) криптографических средств	-	-	-	+	+

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

В криптографической подсистеме для класса 1Б:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на съемные портативные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться принудительная очистка областей внешней памяти, содержавших ранее незашифрованную информацию;
- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;
- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

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

В криптографической подсистеме для класса 1А:

- должно осуществляться шифрование всей конфиденциальной информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;
- должны использоваться разные криптографические ключи для шифрования информации, принадлежащей различным субъектам доступа (группам субъектов);
- доступ субъектов к операциям шифрования и к соответствующим криптографическим ключам должен дополнительно контролироваться посредством подсистемы управления доступом;
- должны использоваться сертифицированные средства криптографической защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации криптографических средств защиты.

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

Подсистемы и требования	Классы				
	1Д	1Г	1В	1Б	1А
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	-	-	+	+	+

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

В подсистеме обеспечения целостности для класса 1Д:

- должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
  - целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- 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.

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

В подсистеме обеспечения целостности для класса 1Г:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
  - целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- 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.

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

В п/системе обеспечения целостности для класса 1В:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ; целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ при обработке и (или) хранении защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;
- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в год;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности;
- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

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

В подсистеме обеспечения целостности для класса 1Б:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется по контрольным суммам всех компонент СЗИ как в процессе загрузки, так и динамически в процессе работы АС;
  - целостность программной среды обеспечивается качеством приемки программных средств в АС, предназначенных для обработки защищенных файлов;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

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

А также в подсистеме обеспечения целостности для класса 1Б:

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ НСД при сбоях;
- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

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

В подсистеме обеспечения целостности для класса 1А:

- должны быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
  - целостность СЗИ НСД проверяется по имитовставкам алгоритма ГОСТ 28147-89 или по контрольным суммам другого аттестованного алгоритма всех компонент СЗИ как в процессе загрузки, так и динамически в процессе функционирования АС;
  - целостность программной среды обеспечивается качеством приемки любых программных средств в АС;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая постоянное наличие охраны территории и здания, где размещается АС, с помощью технических средств охраны и специального персонала, использование строгого пропускного режима, специальное оборудование помещений АС;
- должен быть предусмотрен администратор (служба) защиты информации, ответственный за ведение, нормальное функционирование и контроль работы СЗИ НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС;

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

А также в подсистеме обеспечения целостности для класса 1А:

- должно проводиться периодическое тестирование всех функций СЗИ НСД с помощью специальных программных средств не реже одного раза в квартал;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности, а также автоматическое оперативное восстановление функций СЗИ НСД при сбоях;
- должны использоваться сертифицированные средства защиты. Их сертификацию проводят специальные сертификационные центры или специализированные предприятия, имеющие лицензию на проведение сертификации средств защиты СЗИ НСД.

2. «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации».

Концепция защиты СВТ и АС от НСД к информации

Принятые сокращения

АС - автоматизированная система

КСЗ - комплекс средств защиты

НСД - несанкционированный доступ

ОС - операционная система

ППП - пакет прикладных программ

ПРД - правила разграничения доступа

РД - руководящий документ

СВТ - средства вычислительной техники

СЗИ - система защиты информации

СЗИ НСД - система защиты информации от несанкционированного доступа

СЗСИ - система защиты секретной информации

СНТП - специальное научно-техническое подразделение

СРД - система разграничения доступа

СУБД - система управления базами данных

ТЗ - техническое задание

ЭВМ - электронно-вычислительная машина

ЭВТ - электронно-вычислительная техника

Концепция защиты СВТ и АС от НСД к информации

Определение НСД

НСД определяется как доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых СВТ или АС.

Под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Концепция защиты СВТ и АС от НСД к информации

Общие положения

Концепция является методологической базой нормативно-технических и методических документов, направленных на решение следующих задач:

- выработка требований по защите СВТ и АС от НСД к информации;
- создание защищенных от НСД к информации СВТ и АС;
- сертификация защищенных СВТ и АС.

СВТ разрабатываются и поставляются на рынок лишь как элементы, из которых в дальнейшем строятся функционально ориентированные АС, и поэтому, не решая прикладных задач, СВТ не содержат пользовательской информации.

Помимо пользовательской информации при создании АС появляются такие отсутствующие при разработке СВТ характеристики АС, как полномочия пользователей, модель нарушителя, технология обработки информации.

Концепция защиты СВТ и АС от НСД к информации

В связи с этим, если понятия защищенность (защита) информации от НСД в АС и защищенность (защита) АС от НСД к информации эквивалентны, то в случае СВТ можно говорить лишь о защищенности (защите) СВТ от НСД к информации, для обработки, хранения и передачи которой оно предназначено.

При этом защищенность СВТ есть потенциальная защищенность, т.е. свойство предотвращать или существенно затруднять НСД к информации в дальнейшем при использовании СВТ в АС.

Концепция защиты СВТ и АС от НСД к информации

Основные принципы защиты от НСД

Защита СВТ и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от НСД к информации.

Защита СВТ обеспечивается комплексом программно-технических средств.

Защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер.

Защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ.

Защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Концепция защиты СВТ и АС от НСД к информации

Модель нарушителя в АС

Классификация является иерархической, т.е. каждый следующий уровень включает в себя функциональные возможности предыдущего.

Первый уровень определяет самый низкий уровень возможностей ведения диалога в АС - запуск задач (программ) из фиксированного набора, реализующих заранее предусмотренные функции по обработке информации.

Второй уровень определяется возможностью создания и запуска собственных программ с новыми функциями по обработке информации.

Третий уровень определяется возможностью управления функционированием АС, т.е. воздействием на базовое программное обеспечение системы и на состав и конфигурацию ее оборудования.

Четвертый уровень определяется всем объемом возможностей лиц, осуществляющих проектирование, реализацию и ремонт технических средств АС, вплоть до включения в состав СВТ собственных технических средств с новыми функциями по обработке информации.

В своем уровне нарушитель является специалистом высшей квалификации, знает все об АС и, в частности, о системе и средствах ее защиты.

Концепция защиты СВТ и АС от НСД к информации

Основные способы НСД

К основным способам НСД относятся:

- непосредственное обращение к объектам доступа;
- создание программных и технических средств, выполняющих обращение к объектам доступа в обход средств защиты;
- модификация средств защиты, позволяющая осуществить НСД;
- внедрение в технические средства СВТ или АС программных или технических механизмов, нарушающих предполагаемую структуру и функции СВТ или АС и позволяющих осуществить НСД.

Концепция защиты СВТ и АС от НСД к информации

Основные направления обеспечения защиты от НСД

Обеспечение защиты СВТ и АС осуществляется:

- системой разграничения доступа (СРД) субъектов к объектам доступа;
- обеспечивающими средствами для СРД.

Основными функциями СРД являются:

- реализация правил разграничения доступа (ПРД) субъектов и их процессов к данным;
- реализация ПРД субъектов и их процессов к устройствам создания твердых копий;
- изоляция программ процесса, выполняемого в интересах субъекта, от других субъектов;
- управление потоками данных в целях предотвращения записи данных на носители несоответствующего грифа;
- реализация правил обмена данными между субъектами для АС и СВТ, построенных по сетевым принципам.

Концепция защиты СВТ и АС от НСД к информации

Обеспечивающие средства для СРД выполняют следующие функции:

- идентификацию и опознание (аутентификацию) субъектов и поддержание привязки субъекта к процессу, выполняемому для субъекта;
- регистрацию действий субъекта и его процесса;
- предоставление возможностей исключения и включения новых субъектов и объектов доступа, а также изменение полномочий субъектов;
- реакцию на попытки НСД, например, сигнализацию, блокировку, восстановление после НСД;
- тестирование;
- очистку оперативной памяти и рабочих областей на магнитных носителях после завершения работы пользователя с защищаемыми данными;
- учет выходных печатных и графических форм и твердых копий в АС;
- контроль целостности программной и информационной части как СРД, так и обеспечивающих ее средств.

Концепция защиты СВТ и АС от НСД к информации

Основные характеристики технических средств защиты от НСД

Основными характеристиками технических средств защиты являются:

- степень полноты и качество охвата ПРД реализованной СРД;
- состав и качество обеспечивающих средств для СРД;
- гарантии правильности функционирования СРД и обеспечивающих ее средств.

Оцениваемые АС или СВТ должны быть тщательно документированы. В состав документации включаются Руководство пользователя по использованию защитных механизмов и Руководство по управлению средствами защиты. Для АС и СВТ, претендующих на высокий уровень защищенности, оценка осуществляется при наличии проектной документации (эскизный, технический и рабочий проекты), а также описаний процедур тестирования и их результатов.

Концепция защиты СВТ и АС от НСД к информации

Классификация АС

В основу системы классификации АС должны быть положены следующие характеристики объектов и субъектов защиты, а также способов их взаимодействия:

- информационные, определяющие ценность информации, ее объем и степень (гриф) конфиденциальности, а также возможные последствия неправильного функционирования АС из-за искажения (потери) информации;
- организационные, определяющие полномочия пользователей;
- технологические, определяющие условия обработки информации, например, способ обработки (автономный, мультипрограммный и т.д.), время циркуляции (транзит, хранение и т.д.), вид АС (автономная, сеть, стационарная, подвижная и т.д.).

Концепция защиты СВТ и АС от НСД к информации

Организация работ по защите от НСД

Организация работ по защите СВТ и АС от НСД к информации должна быть частью общей организации работ по безопасности информации.

Обеспечение защиты основывается на требованиях по защите к разрабатываемым СВТ и АС, формулируемых заказчиком и согласуемых с разработчиком.

Эти требования задаются либо в виде желаемого уровня защищенности СВТ или АС, либо в виде определенного, соответствующего этому уровню перечня требований.

Концепция защиты СВТ и АС от НСД к информации

Требования по защите обеспечиваются разработчиком в виде комплекса средств защиты. Организационные мероприятия для АС реализуются заказчиком.

Ответственность за разработку КСЗ возлагается на главного конструктора СВТ или АС.

Проверка выполнения технических требований по защите проводится аналогично с другими техническими требованиями в процессе испытаний (предварительных, государственных и др.).

По результатам успешных испытаний оформляется документ (сертификат), удостоверяющий соответствие СВТ или АС требованиям по защите и дающий право разработчику на использование и (или) распространение их как защищенных.

3. «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации».

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

Под **СВТ** понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

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

Принятые сокращения

АС – автоматизированная система

КД – конструкторская документация

КСЗ – комплекс средств защиты

НСД – несанкционированный доступ

ПРД – правила разграничения доступа

СВТ – средства вычислительной техники

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

Показатели защищенности СВТ применяются к общесистемным программным средствам и операционным системам (с учетом архитектуры ЭВМ).

Конкретные перечни показателей определяют классы защищенности СВТ.

Уменьшение или изменение перечня показателей, соответствующего конкретному классу защищенности СВТ, не допускается.

Каждый показатель описывается совокупностью требований.

Дополнительные требования к показателю защищенности СВТ и соответствие этим дополнительным требованиям оговаривается особо.

Требования к показателям реализуются с помощью программно-технических средств.

Совокупность всех средств защиты составляет комплекс средств защиты.

Документация КСЗ должна быть неотъемлемой частью конструкторской документации на СВТ.

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

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

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.

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

Перечень показателей по классам защищенности СВТ приведен в таблице.

Обозначения:

"-" – нет требований к данному классу;

"**+**" – новые или дополнительные требования;

"=" – требования совпадают с требованиями к СВТ предыдущего класса.

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

Наименование показателя	Класс защищенности					
	6	5	4	3	2	1
Дискреционный принцип контроля доступа	+	+	+	=	+	=
Мандатный принцип контроля доступа	-	-	+	=	=	=
Очистка памяти	-	+	+	+	=	=
Изоляция модулей	-	-	+	=	+	=
Маркировка документов	-	-	+	=	=	=
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=
Сопоставление пользователя с устройством	-	-	+	=	=	=
Идентификация и аутентификация	+	=	+	=	=	=
Гарантии проектирования	-	+	+	+	+	+
Регистрация	-	+	+	+	=	=
Взаимодействие пользователя с КСЗ	-	-	-	+	=	=
Надежное восстановление	-	-	-	+	=	=
Целостность КСЗ	-	+	+	+	=	=
Контроль модификации	-	-	-	-	+	=
Контроль дистрибуции	-	-	-	-	+	=
Гарантии архитектуры	-	-	-	-	-	+
Тестирование	+	+	+	+	+	=
Руководство для пользователя	+	=	=	=	=	=
Руководство по КСЗ	+	+	=	+	+	=
Тестовая документация	+	+	+	+	+	=
Конструкторская (проектная) документация	+	+	+	+	+	+

Приведенные наборы требований к показателям каждого класса являются минимально необходимыми.

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.

1.Требования к показателям защищенности шестого класса

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

1.1. Дискреционный принцип контроля доступа

КСЗ должен контролировать доступ наименованных субъектов (пользователей) к наименованным объектам (файлам, программам, томам и т.д.).

Для каждой пары (субъект – объект) в СВТ должно быть задано явное и недвусмысленное перечисление допустимых типов доступа (читать, писать и т.д.), т.е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу СВТ (объекту).

КСЗ должен содержать механизм, претворяющий в жизнь дискреционные правила разграничения доступа.

Контроль доступа должен быть применим к каждому объекту и каждому субъекту (индивиду или группе равноправных индивидов).

Механизм, реализующий дискреционный принцип контроля доступа, должен предусматривать возможности санкционированного изменения ПРД, в том числе возможность санкционированного изменения списка пользователей СВТ и списка защищаемых объектов.

Права изменять ПРД должны предоставляться выделенным субъектам (администрации, службе безопасности и т.д.).

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

1.2. Идентификация и аутентификация

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ. КСЗ должен подвергать проверке подлинность идентификации – осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации. КСЗ должен препятствовать доступу к защищаемым ресурсам неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

1.3. Тестирование

В СВТ шестого класса должны тестироваться:

- реализация дискреционных ПРД (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.

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

1.4. Руководство для пользователя

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

1.5. Руководство по КСЗ

Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ и процедур проверки правильности старта.

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

1.6. Тестовая документация

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 1.3.) и результатов тестирования.

1.7. Конструкторская (проектная) документация

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

2. Требования к показателям пятого класса защищенности

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

2.1. Дискреционный принцип контроля доступа

Данные требования включает в себя аналогичные требование шестого класса (п.1.1).

Дополнительно должны быть предусмотрены средства управления, ограничивающие распространение прав на доступ.

2.2. Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен предотвращать доступ субъекту к остаточной информации.

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

2.3. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичными требованиями шестого класса (п.1.2).

2.4. Гарантии проектирования

На начальном этапе проектирования СВТ должна быть построена модель защиты. Модель должна включать в себя ПРД к объектам и непротиворечивые правила изменения ПРД.

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

2.5. Регистрация

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.);
- создание и уничтожение объекта;
- действия по изменению ПРД.

Для каждого из этих событий должна регистрироваться следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

КСЗ должен содержать средства выборочного ознакомления с регистрационной информацией.

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

2.6. Целостность КСЗ

В СВТ пятого класса защищенности должны быть предусмотрены средства периодического контроля за целостностью программной и информационной части КСЗ.

2.7. Тестирование

В СВТ пятого класса защищенности должны тестироваться:

- реализация ПРД (перехват явных и скрытых запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов, средства защиты механизма разграничения доступа, санкционированные изменения ПРД);
- успешное осуществление идентификации и аутентификации, а также их средства защиты;
- очистка памяти в соответствии с п. 2.2;
- регистрация событий в соответствии с п. 2.5, средства защиты регистрационной информации и возможность санкционированного ознакомления с ней;
- работа механизма, осуществляющего контроль за целостностью КСЗ.

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

2.8. Руководство пользователя

Данное требование совпадает с аналогичным требованием шестого класса (п. 1.4).

2.9. Руководство по КСЗ

Данный документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описания старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации.

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

2.10. Тестовая документация

Должно быть предоставлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с требованиями п.2.7), и результатов тестирования.

2.11. Конструкторская и проектная документация

Должна содержать:

- описание принципов работы СВТ;
- общую схему КСЗ;
- описание интерфейсов КСЗ с пользователем и интерфейсов модулей КСЗ;
- модель защиты;
- описание механизмов контроля целостности КСЗ, очистки памяти, идентификации и аутентификации.

3. Требования к показателям четвертого класса защищенности

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

3.1. Дискреционный принцип контроля доступа

Данные требования включают аналогичные требования пятого класса (п. 2.1).

Дополнительно КСЗ должен содержать механизм, претворяющий в жизнь дискреционные ПРД, как для явных действий пользователя, так и для скрытых, обеспечивая тем самым защиту объектов от НСД (т.е. от доступа, не допустимого с точки зрения заданного ПРД). Под "явными" здесь подразумеваются действия, осуществляемые с использованием системных средств - системных макрокоманд, инструкций языков высокого уровня и т.д., а под "скрытыми" - иные действия, в том числе с использованием собственных программ работы с устройствами.

Дискреционные ПРД для систем данного класса являются дополнением мандатных ПРД.

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

3.2. Мандатный принцип контроля доступа

Для реализации этого принципа должны сопоставляться классификационные метки каждого субъекта и каждого объекта, отражающие их место в соответствующей иерархии. Посредством этих меток субъектам и объектам должны назначаться классификационные уровни (уровни уязвимости, категории секретности и т.п.), являющиеся комбинациями иерархических и неиерархических категорий. Данные метки должны служить основой мандатного принципа разграничения доступа.

КСЗ при вводе новых данных в систему должен запрашивать и получать от санкционированного пользователя классификационные метки этих данных. При санкционированном занесении в список пользователей нового субъекта должно осуществляться сопоставление ему классификационных меток. Внешние классификационные метки (субъектов, объектов) должны точно соответствовать внутренним меткам (внутри КСЗ).

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

3.2. Мандатный принцип контроля доступа

КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам при явном и скрытом доступе со стороны любого из субъектов:

- субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;
- субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются в неиерархические категории в классификационном уровне объекта.

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

3.2. Мандатный принцип контроля доступа

Реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами.

В СВТ должен быть реализован диспетчер доступа, т.е. средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа. При этом решение о санкционированности запроса на доступ должно приниматься только при одновременном разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

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

3.3. Очистка памяти

При первоначальном назначении или при перераспределении внешней памяти КСЗ должен затруднять субъекту доступ к остаточной информации. При перераспределении оперативной памяти КСЗ должен осуществлять ее очистку.

3.4. Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть защищены друг от друга.

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

3.5. Маркировка документов

При выводе защищаемой информации на документ в начале и конце проставляют штамп № 1 и заполняют его реквизиты в соответствии с Инструкцией № 0126-87 (п. 577).

3.6. Защита ввода и вывода на отчуждаемый физический носитель информации

КСЗ должен различать каждое устройство ввода-вывода и каждый канал связи как произвольно используемые или идентифицированные ("помеченные"). При вводе с "помеченного" устройства (вывода на "помеченное" устройство) КСЗ должен обеспечивать соответствие между меткой вводимого (выводимого) объекта (классификационным уровнем) и меткой устройства. Такое же соответствие должно обеспечиваться при работе с "помеченным" каналом связи.

Изменения в назначении и разметке устройств и каналов должны осуществляться только под контролем КСЗ.

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

3.7. Сопоставление пользователя с устройством

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентифицированный КСЗ должен включать в себя механизм, посредством которого санкционированный пользователь надежно сопоставляется выделенному устройству.

3.8. Идентификация и аутентификация

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта - осуществлять аутентификацию. КСЗ должен располагать необходимыми данными для идентификации и аутентификации и препятствовать входу в СВТ неидентифицированного пользователя или пользователя, чья подлинность при аутентификации не подтвердилась.

КСЗ должен обладать способностью надежно связывать полученную идентификацию со всеми действиями данного пользователя.

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

3.9. Гарантии проектирования

Проектирование КСЗ должно начинаться с построения модели защиты, содержащей:
- непротиворечивые ПРД;
- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода информации и каналами связи.

3.10. Регистрация

Данные требования включают аналогичные требования пятого класса защищенности (п.2.5). Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей (администраторов защиты и т.п.).

3.11. Целостность КСЗ

В СВТ четвертого класса защищенности должен осуществляться периодический контроль за целостностью КСЗ.

Программы КСЗ должны выполняться в отдельной части оперативной памяти.

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

3.12. Тестирование

В четвертом классе защищенности должны тестироваться:

• реализация ПРД (перехват запросов на доступ, правильное распознавание санкционированных и несанкционированных запросов в соответствии с дискреционными и мандатными правилами, верное сопоставление меток субъектов и объектов, запрос меток вновь вводимой информации, средства защиты механизма разграничения доступа, санкционированное изменение ПРД);

• невозможность присвоения субъектом себе новых прав;

• очистка оперативной и внешней памяти;

• работа механизма изоляции процессов в оперативной памяти;

• маркировка документов;

• защита вода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством;

• идентификация и аутентификация, а также их средства защиты;

• запрет на доступ несанкционированного пользователя;

• работа механизма, осуществляющего контроль за целостностью СВТ;

• регистрация событий, описанных в п. 3.10, средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией.

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

3.13. Руководство для пользователя

Данное требование совпадает с аналогичным требованием шестого (п. 1.4) и пятого (п. 2.8) классов.

3.14. Руководство по КСЗ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 2.9).

3.15. Тестовая документация

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (в соответствии с п. 3.12) и результатов тестирования.

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

3.16. Конструкторская (проектная) документация

Должна содержать:

- общее описание принципов работы СВТ;
- общую схему КСЗ;
- описание внешних интерфейсов КСЗ и интерфейсов модулей КСЗ;
- описание модели защиты;
- описание диспетчера доступа;
- описание механизма контроля целостности КСЗ;
- описание механизма очистки памяти;
- описание механизма изоляции программ в оперативной памяти;
- описание средств защиты ввода и вывода на отчуждаемый физический носитель информации и сопоставления пользователя с устройством;
- описание механизма идентификации и аутентификации;
- описание средств регистрации.

4. Требования к показателям третьего класса защищенности

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

4.1. Дискреционный принцип контроля доступа

Данные требования полностью совпадают с требованиями пятого (п. 2.1) и четвертого классов (п. 3.1).

4.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.2).

4.3. Очистка памяти

Для СВТ третьего класса защищенности КСЗ должен осуществлять очистку оперативной и внешней памяти. Очистка должна производиться путем записи маскирующей информации в память при ее освобождении (перераспределении).

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

4.4. Изоляция модулей

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.4).

4.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.5).

4.6. Защита ввода и вывода на отчуждаемый физический носитель информации

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.6).

4.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.7).

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

4.8. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.8).

4.9. Гарантии проектирования

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом. Эта модель должна содержать:

- непротиворечивые правила изменения ПРД;
- правила работы с устройствами ввода и вывода;
- формальную модель механизма управления доступом.

Должна предлагаться высокоуровневая спецификация части КСЗ, реализующего механизм управления доступом и его интерфейсов. Эта спецификация должна быть верифицирована на соответствие заданных принципов разграничения доступа.

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

4.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.10).

4.11. Взаимодействие пользователя с КСЗ

Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

4.12. Надежное восстановление

Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

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

4.13. Целостность КСЗ

Необходимо осуществлять периодический контроль за целостностью КСЗ.

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

4.14. Тестирование

СВТ должны подвергаться такому же тестированию, что и СВТ четвертого класса (п. 3.12).

Дополнительно должны тестироваться:

- очистка памяти (п. 4.3);
- работа механизма надежного восстановления.

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

4.15. Руководство для пользователя

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п. 3.13).

4.16. Руководство по КСЗ

Документ адресован администратору защиты и должен содержать:

- описание контролируемых функций;
- руководство по генерации КСЗ;
- описание старта СВТ, процедур проверки правильности старта, процедур работы со средствами регистрации;
- руководство по средствам надежного восстановления.

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

4.17. Тестовая документация

В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п. 4.14), а также результатов тестирования.

4.18. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ четвертого класса (п.3.16).

Дополнительно необходимы:

- высокоуровневая спецификация КСЗ и его интерфейсов;
- верификация соответствия высокоуровневой спецификации КСЗ модели защиты.

5. Требования к показателям второго класса защищенности.

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

5.1. Дискреционный принцип контроля доступа

Данные требования включают аналогичные требования третьего класса (п.4.1).

Дополнительно требуется, чтобы дискреционные правила разграничения доступа были эквивалентны мандатным правилам (т.е. всякий запрос на доступ должен быть одновременно санкционированным или несанкционированным одновременно и по дискреционным правилам, и по мандатным ПРД).

5.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 4.2).

5.3. Очистка памяти

Данные требования полностью совпадают с аналогичным требованием третьего класса (п. 4.3).

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

5.4. Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно-технический механизм, изолирующий программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов) - т.е. в оперативной памяти ЭВМ программы разных пользователей должны быть изолированы друг от друга. Гарантии изоляции должны быть основаны на архитектуре СВТ.

5.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием четвертого класса (п.4.5).

5.6. Защита ввода и вывода на отчуждаемый физический носитель информации

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.4.6).

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

5.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием четвертого (п.3.7) и третьего (п.4.7) классов.

5.8. Идентификация и аутентификация

Требование полностью совпадает с аналогичным требованием четвертого (п.3.8) и третьего (п.4.8) классов.

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

5.9. Гарантии проектирования

Данные требования включают аналогичные требования третьего класса (п.4.9).

Дополнительно требуется, чтобы высокоуровневые спецификации КСЗ были отображены последовательно в спецификации одного или нескольких нижних уровней, вплоть до реализации высокоуровневой спецификации КСЗ на языке программирования высокого уровня. При этом методами верификации должно осуществляться доказательство соответствия каждого такого отображения спецификациям высокого (верхнего для данного отображения) уровня. Этот процесс может включать в себя как одно отображение (высокоуровневая спецификация - язык программирования), так и последовательность отображений в промежуточные спецификации с понижением уровня, вплоть до языка программирования. В результате верификации соответствия каждого уровня предыдущему должно достигаться соответствие реализации высокоуровневой спецификации КСЗ модели защиты, изображенной на чертеже.

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

5.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием четвертого (п.3.10) и третьего (п.4.10) классов.

5.11. Взаимодействие пользователя с КСЗ

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.4.11).

5.12. Надежное восстановление

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.4.12).

5.13. Целостность КСЗ

Данные требования полностью совпадают с аналогичным требованием третьего класса (п.4.13).

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

5.14. Контроль модификации

При проектировании, построении и сопровождении СВТ должно быть предусмотрено управление конфигурацией СВТ, т.е. контроль изменений в формальной модели, спецификациях (разных уровней), документации, исходном тексте, версии в объектном коде. Должно обеспечиваться соответствие между документацией и текстами программ. Должна осуществляться сравниваемость генерируемых версий. Оригиналы программ должны быть защищены.

5.15. Контроль дистрибуции

Должен осуществляться контроль точности копирования в СВТ при изготовлении копий с образца. Изготовляемая копия должна гарантированно повторять образец

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

5.16. Тестирование

СВТ второго класса должны тестироваться так же, как и СВТ третьего класса (п.4.14).

Дополнительно должен тестироваться контроль дистрибуции.

5.17. Руководство для пользователя

Данные требования полностью совпадают с аналогичным требованием четвертого (п.3.13) и третьего (п.4.15) классов.

5.18. Руководство по КСЗ

Данные требования включают аналогичные требования третьего класса (п. 4.16).

Дополнительно должны быть представлены руководства по надежному восстановлению, по работе со средствами контроля модификации и дистрибуции.

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

5.19. Тестовая документация

Должно быть представлено описание тестов и испытаний, которым подвергалось СВТ (п.5.16), а также результатов тестирования.

5.20. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ третьего класса (п.4.18).

Дополнительно должны быть описаны гарантии процесса проектирования и эквивалентность дискреционных (п.5.1) и мандатных (п.5.2) ПРД.

6. Требования к показателям первого класса защищенности

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

6.1. Дискреционный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.1).

6.2. Мандатный принцип контроля доступа

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.2).

6.3. Очистка памяти

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.3).

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

6.4. Изоляция модулей

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.4).

6.5. Маркировка документов

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.5).

6.6. Защита ввода и вывода на отчуждаемый физический носитель информации

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.6).

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

6.7. Сопоставление пользователя с устройством

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.7).

6.8. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.8).

6.9. Гарантии проектирования

Данные требования включают аналогичные требования второго класса (п.5.9).

Дополнительно требуется верификация соответствия объектного кода тексту КСЗ на языке высокого уровня.

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

6.10. Регистрация

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.10).

6.11. Взаимодействие пользователя с КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.11).

6.12. Надежное восстановление

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.12).

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

6.13. Целостность КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.13).

6.14. Контроль модификации

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.14).

6.15. Контроль дистрибуции

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.15).

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

6.16. Гарантии архитектуры

КСЗ должен обладать механизмом, гарантирующим перехват диспетчером доступа всех обращений субъектов к объектам.

6.17. Тестирование

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.16).

6.18. Руководство пользователя

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.17).

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

6.19. Руководство по КСЗ

Данные требования полностью совпадают с аналогичным требованием второго класса (п.5.18).

6.20. Тестовая документация

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.5.19).

6.21. Конструкторская (проектная) документация

Требуется такая же документация, что и для СВТ второго класса (п.5.20). Дополнительно разрабатывается описание гарантий процесса проектирования (п.6.9).

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

Оценка класса защищенности СВТ (сертификация СВТ)

Оценка класса защищенности СВТ проводится в соответствии с Положением о сертификации средств и систем вычислительной техники и связи по требованиям защиты информации, Временным положением по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники и другими документами.

4. Средства вычислительной техники. Межсетевые экраны
Защита от несанкционированного доступа к информации
Показатели защищенности от несанкционированного доступа к информации.

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

Руководящий документ разработан в дополнение к Руководящим документам Гостехкомиссии России “Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации” и “Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации”.

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

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.

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

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.

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

Термины и определения

Администратор МЭ - лицо, ответственное за сопровождение МЭ.

Дистанционное управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ с узла (рабочей станции) сети, на котором не функционирует МЭ (компонента) с использованием сетевых протоколов.

Критерии фильтрации - параметры, атрибуты, характеристики, на основе которых осуществляется разрешение или запрещение дальнейшей передачи пакета (данных) в соответствии с заданными правилами разграничения доступа (правилами фильтрации). В качестве таких параметров могут использоваться служебные поля пакетов (данных), содержащие сетевые адреса, идентификаторы, адреса интерфейсов, портов и другие значимые данные, а также внешние характеристики, например, временные, частотные характеристики, объем данных и т.п.

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

Термины и определения

Локальное (местное) управление компонентами МЭ - выполнение функций по сопровождению МЭ (компоненты) администратором МЭ на том же узле (платформе), на котором функционирует МЭ (компонента) с использованием интерфейса МЭ.

Межсетевой экран (МЭ) - это локальное (однокомпонентное) или функционально - распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в АС и/или выходящей из АС. МЭ обеспечивает защиту АС посредством фильтрации информации, т.е. ее анализа по совокупности критериев и принятия решения о ее распространении в (из) АС на основе заданных правил, проводя таким образом разграничение доступа субъектов из одной АС к объектам другой АС. Каждое правило запрещает или разрешает передачу информации определенного вида между субъектами и объектами. Как следствие, субъекты из одной АС получают доступ только к разрешенным информационным объектам из другой АС. Интерпретация набора правил выполняется последовательностью фильтров, которые разрешают или запрещают передачу данных (пакетов) на следующий фильтр или уровень протокола.

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

Термины и определения

Правила фильтрации - перечень условий по которым с использованием заданных критериев фильтрации осуществляется разрешение или запрещение дальнейшей передачи пакетов (данных) и перечень действий, производимых МЭ по регистрации и/или осуществлению дополнительных защитных функций.

Межсетевой экран может строиться с помощью экранирующих агентов, которые обеспечивают установление соединения между субъектом и объектом, а затем пересылают информацию, осуществляя контроль и/или регистрацию. Использование экранирующих агентов позволяет предоставить дополнительную защитную функцию - сокрытие от субъекта истинного объекта. В то же время, субъекту кажется, что он непосредственно взаимодействует с объектом. Обычно экран не является симметричным, для него определены понятия "внутри" и "снаружи". При этом задача экранирования формулируется как защита внутренней области от неконтролируемой и потенциально враждебной внешней.

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

Термины и определения

Сетевые адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом сетевого уровня модели международной организации по стандартизации взаимодействия открытых систем (ISO OSI).

Сетевой протокол выполняет управление коммуникационными ресурсами, маршрутизацию пакетов, их компоновку для передачи в сети. В этих протоколах решается возможность доступа к подсети, определяется маршрут передачи и осуществляется трансляция сообщения. Управление доступом на сетевом уровне позволяет отклонять нежелательные вызовы и дает возможность различным подсетям управлять использованием ресурсов сетевого уровня. Поэтому, в данных протоколах возможно выполнение требований по защите в части проверки подлинности сетевых ресурсов, источника и приемника данных, принимаемых сообщений, проведения контроля доступа к ресурсам сети.

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

Термины и определения

Трансляция адреса - функция МЭ, скрывающая внутренние адреса объектов (субъектов) от внешних субъектов.

Транспортные адреса - адресные данные, идентифицирующие субъекты и объекты и используемые протоколом транспортного уровня модели ISO OSI. Протоколы транспортного уровня обеспечивают создание и функционирование логических каналов между программами (процессами, пользователями) в различных узлах сети, управляют потоками информации между портами, осуществляют компоновку пакетов о запросах и ответах.

Централизованное управление компонентами МЭ - выполнение с одного рабочего места (рабочей станции, узла) всех функций по сопровождению МЭ (его компонент), только со стороны санкционированного администратора, включая инициализацию, останов, восстановление, тестирование, установку и модификацию правил фильтрации данных, параметров регистрации, дополнительных защитных функций и анализ зарегистрированных событий.

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

Термины и определения

Экранирование - функция МЭ, позволяющая поддерживать безопасность объектов внутренней области, игнорируя несанкционированные запросы из внешней области.

В результате экранирования уменьшается уязвимость внутренних объектов, поскольку первоначально сторонний нарушитель должен преодолеть экран, где защитные механизмы сконфигурированы особенно тщательно и жестко. Кроме того, экранирующая система, в отличие от универсальной, может и должна быть устроена более простым и, следовательно, более безопасным образом, на ней должны присутствовать только те компоненты, которые необходимы для выполнения функций экранирования.

Экранирование дает также возможность контролировать информационные потоки, направленные во внешнюю область, что способствует поддержанию во внутренней области режима конфиденциальности.

Помимо функций разграничения доступа, экраны осуществляют регистрацию информационных обменов.

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

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	+	=	+	=	+

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

1.Требования к пятому классу защищенности МЭ

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

1.1. 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.

1.2. 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.

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

1.3. Администрирование: регистрация

МЭ должен обеспечивать регистрацию входа (выхода) администратора МЭ в систему (из системы) либо загрузки и инициализации системы и ее программного останова. Регистрация выхода из системы не проводится в моменты аппаратурного отключения МЭ.

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.

1.4. Целостность

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

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

1.5. Восстановление

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

1.6. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:
•реализации правил фильтрации (см. п. 1.1);
•процесса идентификации и аутентификации администратора МЭ (см. п. 1.2);
•процесса регистрации действий администратора МЭ (см. п. 1.3.);
•процесса контроля за целостностью программной и информационной части МЭ (см. п.1.4);
•процедуры восстановления (см. п. 1.5.).

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

1.7. 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.

1.8. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 1.6), и результаты тестирования.

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

1.9. 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.

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

2. Требования к четвертому классу защищенности МЭ

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

2.1. Управление доступом

Данные требования полностью включают аналогичные требования пятого класса (п.1.1).

Дополнительно МЭ должен обеспечивать:

- фильтрацию пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;
- фильтрацию с учетом входного и выходного сетевого интерфейса как средство проверки подлинности сетевых адресов;
- фильтрацию с учетом любых значимых полей сетевых пакетов.

2.2. Регистрация

МЭ должен обеспечивать возможность регистрации и учета фильтруемых пакетов. В параметры регистрации включаются адрес, время и результат фильтрации.

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

2.3. Администрирование: идентификация и аутентификация

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.2).

2.4. Администрирование: регистрация

Данные требования включают аналогичные требования пятого класса (п.1.3).

Дополнительно МЭ должен обеспечивать регистрацию запуска программ и процессов (заданий, задач).

2.5. Целостность

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.4).

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

2.6. Восстановление

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.5).

2.7. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:
•реализации правил фильтрации (см. п. 2.1);
•процесса регистрации (см. п. 2.2);
•процесса идентификации и аутентификации администратора МЭ (см. п. 2.3);
•процесса регистрации действий администратора МЭ (см. п. 2.4);
•процесса контроля за целостностью программной и информационной части МЭ (см. п.2.5);
•процедуры восстановления (см. п. 2.6).

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

2.8. Руководство администратора МЭ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 1.7).

2.9. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 2.7), и результаты тестирования.

2.10. Конструкторская (проектная) документация

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п. 1.9) по составу документации.

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

3. Требования к третьему классу защищенности МЭ

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

3.1. Управление доступом

Данные требования полностью включают аналогичные требования четвертого класса (п. 2.1).

Дополнительно МЭ должен обеспечивать:
•фильтрацию на транспортном уровне запросов на установление виртуальных соединений. При этом, по крайней мере, учитываются транспортные адреса отправителя и получателя;
•фильтрацию на прикладном уровне запросов к прикладным сервисам. При этом, по крайней мере, учитываются прикладные адреса отправителя и получателя;
•фильтрацию с учетом даты/времени.

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

3.2. Идентификация и аутентификация

МЭ должен обеспечивать возможность аутентификации входящих и исходящих запросов методами, устойчивыми к пассивному и/или активному прослушиванию сети.

3.3. Регистрация

Данные требования включают аналогичные требования четвертого класса (п.2.2).

Дополнительно МЭ должен обеспечивать:
- регистрацию и учет запросов на установление виртуальных соединений;
- локальную сигнализацию попыток нарушения правил фильтрации.

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

3.4. Администрирование: идентификация и аутентификация

Данные требования включают аналогичные требования пятого класса (п.1.2).

Дополнительно МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах администратора МЭ на доступ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

3.5. Администрирование: регистрация

Данные требования полностью включают аналогичные требования четвертого класса (п.2.4).

Дополнительно МЭ должен обеспечивать регистрацию действия администратора МЭ по изменению правил фильтрации.

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

3.6. Администрирование: простота использования

Многокомпонентный МЭ должен обеспечивать возможность дистанционного управления своими компонентами, в том числе, возможность конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

3.7. Целостность

Данные требования полностью включают аналогичные требования пятого класса (п.1.4).

Дополнительно должен обеспечиваться контроль целостности программной и информационной части МЭ по контрольным суммам.

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

3.8. Восстановление

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.5).

3.9. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:
•реализации правил фильтрации (см. п. 3.1);
•процесса регистрации (см. п. 3.3);
•процесса идентификации и аутентификации запросов (см. п. 3.2);
•процесса идентификации и аутентификации администратора МЭ (см. п. 3.4);
•процесса регистрации действий администратора МЭ (см. п. 3.5);
•процесса контроля за целостностью программной и информационной части МЭ (см. п. 3.7);
•процедуры восстановления (см. п. 3.8.).

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

3.10. Руководство администратора МЭ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.7).

3.11. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 3.9), и результаты тестирования.

3.12. Конструкторская (проектная) документация

Данные требования полностью включают аналогичные требования пятого класса (п. 1.9) по составу документации.

Дополнительно документация должна содержать описание средств и процесса централизованного управления компонентами МЭ.

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

4. Требования ко второму классу защищенности МЭ

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

4.1. Управление доступом

Данные требования включают аналогичные требования третьего класса (п.3.1).

Дополнительно МЭ должен обеспечивать:

•возможность сокрытия субъектов (объектов) и/или прикладных функций защищаемой сети;

•возможность трансляции сетевых адресов.

4.2. Идентификация и аутентификация

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.3.2).

4.3. Регистрация

Данные требования включают аналогичные требования третьего класса (п.3.3).

Дополнительно МЭ должен обеспечивать:

•дистанционную сигнализацию попыток нарушения правил фильтрации;

•регистрацию и учет запрашиваемых сервисов прикладного уровня;

•программируемую реакцию на события в МЭ.

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

4.4. Администрирование: идентификация и аутентификация

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по идентификатору (коду) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

4.5. Администрирование: регистрация

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.3.5).

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

4.6. Администрирование: простота использования

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.3.6).

4.7. Целостность

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам как в процессе загрузки, так и динамически.

4.8. Восстановление

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

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

4.9. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования
•реализации правил фильтрации (см. п. 4.1);
•процесса идентификации и аутентификации (см. п. 4.2);
•процесса регистрации (см. п. 4.3);
•процесса идентификации и аутентификации администратора МЭ (см. п. 4.4);
•процесса регистрации действий администратора МЭ (см. п. 4.5);
•процесса контроля за целостностью программной и информационной части МЭ (см. п. 4.7);
•процедуры восстановления (см. п. 4.8).

4.10. Руководство администратора МЭ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.7).

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

4.11. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 4.9), и результаты тестирования.

4.12. Конструкторская (проектная) документация

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п. 3.12) по составу документации.

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

5. Требования к первому классу защищенности МЭ

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

5.1. Управление доступом

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.4.1).

5.2. Идентификация и аутентификация

Данные требования полностью включают аналогичные требования второго класса (п.4.2).

Дополнительно МЭ должен обеспечивать идентификацию и аутентификацию всех субъектов прикладного уровня.

5.3. Регистрация

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.4.3).

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

5.4. Администрирование: идентификация и аутентификация

МЭ должен обеспечивать идентификацию и аутентификацию администратора МЭ при его запросах на доступ. МЭ должен предоставлять возможность для идентификации и аутентификации по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия. МЭ должен препятствовать доступу неидентифицированного субъекта или субъекта, подлинность идентификации которого при аутентификации не подтвердилась.

При удаленных запросах на доступ администратора МЭ идентификация и аутентификация должны обеспечиваться методами, устойчивыми к пассивному и активному перехвату информации.

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

5.5. Администрирование: регистрация

Данные требования полностью совпадают с аналогичными требованиями третьего класса (п.3.5).

5.6. Администрирование: простота использования

Многокомпонентный МЭ должен обеспечивать возможность централизованного управления своими компонентами, в том числе, конфигурирования фильтров, проверки взаимной согласованности всех фильтров, анализа регистрационной информации.

Должен быть предусмотрен графический интерфейс для управления МЭ.

5.7. Целостность

МЭ должен содержать средства контроля за целостностью своей программной и информационной части по контрольным суммам аттестованного алгоритма как в процессе загрузки, так и динамически.

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

5.8. Восстановление

Данные требования полностью совпадают с аналогичными требованиями второго класса (п.4.8).

5.9. Тестирование

В МЭ должна обеспечиваться возможность регламентного тестирования:
- реализации правил фильтрации (см. п. 5.1);
- процесса идентификации и аутентификации (см. п. 5.2);
- процесса регистрации (см. п. 5.3);
- процесса идентификации и аутентификации администратора МЭ (см. п. 5.4);
- процесса регистрации действий администратора МЭ (см. п. 5.5);
- процесса централизованного управления компонентами МЭ и графический интерфейс для управления МЭ (см. п. 5.6);
- процесса контроля за целостностью программной и информационной части МЭ (см. п. 5.7);
- процедуры восстановления (см. п. 5.8).

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

5.10. Руководство администратора МЭ

Данные требования полностью совпадают с аналогичными требованиями пятого класса (п.1.7).

5.11. Тестовая документация

Должна содержать описание тестов и испытаний, которым подвергался МЭ (в соответствии с п. 5.9), и результаты тестирования.

5.12. Конструкторская (проектная) документация

Данные требования полностью включают аналогичные требования третьего класса (п. 3.12) по составу документации.

Дополнительно документация должна содержать описание графического интерфейса для управления МЭ.