ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Руководящий документ

АВТОМАТИЗИРОВАННЫЕ СИСТЕМЫ
ЗАЩИТА ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К ИНФОРМАЦИИ.
КЛАССИФИКАЦИЯ АВТОМАТИЗИРОВАННЫХ СИСТЕМ И ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ

Москва – 1992

Руководящий документ Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». – М.: ГТК РФ, 1992. – 39 с.

Настоящий руководящий документ устанавливает классификацию автоматизированных систем, подлежащих защите от несанкционированного доступа к информации, и требования по защите информации в АС различных классов.

Руководящий документ разработан в дополнение ГОСТ 34.003-90, ГОСТ 34.601-90, РД 50-680-88, РД 50-34.680-90 и других документов.

Документ может использоваться как нормативно-методический материал для заказчиков и разработчиков АС при формулировании и реализации требований по защите.

Принятые сокращения

АС - автоматизированные системы

НСД - несанкционированный доступ

РД - руководящий документ

СЗИ - система защиты информации

СЗИ НСД - система защиты информации от несанкционированного доступа

1. КЛАССИФИКАЦИЯ АС

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

1.2. Деление АС на соответствующие классы по условиям их функционирования с точки зрения защиты информации необходимо в целях разработки и применения обоснованных мер по достижению требуемого уровня защиты информации.

1.3. Дифференциация подхода к выбору методов и средств защиты определяется важностью обрабатываемой информации, различием АС по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

1.4. 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.

1.5. 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.

1.6. Выбор класса АС производится заказчиком и разработчиком с

привлечением специалистов по защите информации.

1.7. К числу определяющих признаков, по которым производится группировка АС в различные классы, относятся:

наличие в АС информации различного уровня конфиденциальности;

уровень полномочий субъектов доступа АС на доступ к конфиденциальной информации;

режим обработки данных в АС - коллективный или индивидуальный.

1.8. Устанавливается девять классов защищенности АС от НСД к информации.

Каждый класс характеризуется определенной минимальной совокупностью требований по защите.

Классы подразделяются на три группы, отличающиеся особенностями обработки информации в АС.

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

1.9. 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.

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.

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.

2. ТРЕБОВАНИЯ ПО ЗАЩИТЕ ИНФОРМАЦИИ ОТ НСД ДЛЯ АС

2.1. Защита информации от НСД является составной частью общей проблемы обеспечения безопасности информации. Мероприятия по защите информации от НСД должны осуществляться взаимосвязано с мероприятиями по специальной защите основных и вспомогательных средств вычислительной техники, средств и систем связи от технических средств разведки и промышленного шпионажа.

2.2. 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.

2.3. В зависимости от класса АС в рамках этих подсистем должны быть реализованы требования в соответствии с пп. 2.4, 2.7 и 2.10. Подробно эти требования сформулированы в пп. 2.5, 2.6, 2.8, 2.9 и 2.11-2.15.

2.4. Требования к АС третьей группы

Обозначения:

« - » - нет требований к данному классу;

« + » - есть требования к данному классу.

Подсистемы и требования	Классы	
	3А	3Б
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		

в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	-
к программам	-	-
к томам, каталогам, файлам, записям, полям записей	-	-
1.2. Управление потоками информации	-	-
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) системы (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	-	-
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	-	-

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	-	+

Подсистема регистрации и учета:

- 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;

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

Подсистема обеспечения целостности:

- 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;

- 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.

2.6. Требования к классу защищенности 3А:

Подсистема управления доступом:

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

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

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

- 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];

- должен проводиться учет всех защищаемых носителей информации

с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);

- 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).

Подсистема обеспечения целостности:

- 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;

- 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.

2.7. Требования к АС второй группы

Обозначения:

« - » - нет требований к данному классу;

« + » - есть требования к данному классу.

Подсистемы и требования	**Классы**	
	2А	**2Б**
1. Подсистема управления доступом		
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:		
в систему	+	+
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	-	+
к программам	-	+
к томам, каталогам, файлам, записям, полям записей	-	+
1.2. Управление потоками информации	-	+
2. Подсистема регистрации и учета		
2.1. Регистрация и учет:		
входа (выхода) субъектов доступа в (из) системы (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	-	-
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	-	+
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	-	+

2.8. Требования к классу защищенности 2Б:

Подсистема управления доступом:

- 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.

Подсистема регистрации и учета:

- 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).

Подсистема обеспечения целостности:

- 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.

2.9. Требования к классу защищенности 2А.

Подсистема управления доступом:

- 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 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.

Подсистема регистрации и учета:

- 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);

- 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)];

- 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).

Криптографическая подсистема:

- 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.

Подсистема обеспечения целостности:

- 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.

2.10. Требования к АС первой группы

Обозначения:

« - » - нет требований к данному классу;

« + » - есть требования к данному классу.

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	-	-	+	+	+
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	-	-	+	+	+
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	-	-	-	+	+
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	-	-	+	+	+

Подсистема регистрации и учета:

- 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 в журнал (учетную карточку);

- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Подсистема обеспечения целостности:

- 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.

2.12. Требования к классу защищенности 1Г:

Подсистема управления доступом:

- 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.

Подсистема регистрации и учета:

- 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;

- 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;

- 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);

- 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)];

- 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);

Подсистема обеспечения целостности:

- 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.

2.13. Требования к классу защищенности 1В:

Подсистема управления доступом:

- 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.

Подсистема регистрации и учета:

- 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;

- 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;

- 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);

- 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.);

- 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.);

- 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;

- 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;

- 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.

Подсистема обеспечения целостности:

- 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.

2.14. Требования к классу защищенности 1Б:

Подсистема управления доступом:

- 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.

Подсистема регистрации и учета:

- 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;

- 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;

- 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.);

- 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.);

- 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;

- 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.

Криптографическая подсистема:

- 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.

Подсистема обеспечения целостности:

- 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;

- 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.

2.15. Требования к классу защищенности 1А:

Подсистема управления доступом:

- 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.

Подсистема регистрации и учета:

- 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;

- 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;

- 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.);

- 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.);

- 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;

- 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.

Криптографическая подсистема:

- 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.

Подсистема обеспечения целостности:

- 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;

- 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.

2.16. Организационные мероприятия в рамках СЗИ НСД в АС, обрабатывающих или хранящих информацию, являющуюся собственностью государства и отнесенную к категории секретной, должны отвечать государственным требованиям по обеспечению режима секретности проводимых работ.

2.17. При обработке или хранении в АС информации, не отнесенной к категории секретной, в рамках СЗИ НСД государственным, коллективным, частным и совместным предприятиям, а также частным лицам рекомендуются следующие организационные мероприятия:

выявление конфиденциальной информации и ее документальное оформление в виде перечня сведений, подлежащих защите;

определение порядка установления уровня полномочий субъекта доступа, а также круга лиц, которым это право предоставлено;

установление и оформление правил разграничения доступа, т.е. совокупности правил, регламентирующих права доступа субъектов к объектам;

ознакомление субъекта доступа с перечнем защищаемых сведений и его уровнем полномочий, а также с организационно-распорядительной и рабочей документацией, определяющей требования и порядок обработки конфиденциальной информации;

получение от субъекта доступа расписки о неразглашении доверенной ему конфиденциальной информации;

обеспечение охраны объекта, на котором расположена защищаемая АС, (территория, здания, помещения, хранилища информационных носителей) путем установления соответствующих постов, технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими хищение средств вычислительной техники (СВТ), информационных носителей, а также НСД к СВТ и линиям связи;

выбор класса защищенности АС в соответствии с особенностями обработки информации (технология обработки, конкретные условия эксплуатации АС) и уровнем ее конфиденциальности;

организация службы безопасности информации (ответственные лица, администратор АС), осуществляющей учет, хранение и выдачу информационных носителей, паролей, ключей, ведение служебной информации СЗИ НСД (генерацию паролей, ключей, сопровождение правил разграничения доступа), приемку включаемых в АС новых программных средств, а также контроль за ходом технологического процесса обработки конфиденциальной информации и т.д.;

разработка СЗИ НСД, включая соответствующую организационно-распорядительную и эксплуатационную документацию;

осуществление приемки СЗИ НСД в составе АС.

2.18. При разработке АС, предназначенной для обработки или хранения информации, являющейся собственностью государства и отнесенной к категории секретной, необходимо ориентироваться в соответствии с РД «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» на классы защищенности АС не ниже (по группам) 3А, 2А, 1А, 1Б, 1В и использовать сертифицированные СВТ:

не ниже 4 класса - для класса защищенности АС 1В;

не ниже 3 класса - для класса защищенности АС 1Б;

не ниже 2 класса - для класса защищенности АС 1А.