Закрытие пунктов РД АС до 1Б

Дата экспорта 23 ноября 2020
v1

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
1	Подсистема управления доступом:			
1.1	Идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов	Проверка возможностей системы защиты АС по идентификации и проверки подлинности субъектов доступа при входе в автоматизированную систему по идентификатору (коду) и паролю временного действия длиной не менее восьми буквенно-цифровых символов	В ходе проверки проводится анализ установленных параметров осуществления идентификации и аутентификации. Определяются установленные значения для следующих параметров: минимальная длина пароля; сложность пароля; максимальный срок действия пароля. В случае если указанные параметры не определены осуществляется проверка организационных мероприятий, которые позволяют АС выполнить необходимые требования к классу защищенности 1Б у администратора информационной безопасности АС должны быть в наличии нормативные документы, в которых регламентирован порядок реализации защиты с помощью паролей в данной АС. В нормативных документах должны быть указаны требования к паролям, аналогичные приведенным выше, обязанности администратора по реализации требований к защите паролем в рассматриваемой АС и т. д. Далее, для проверки корректности осуществления идентификации и аутентификации в данной АС, произвольным образом выбирается несколько учетных записей пользователей. Для каждой выбранной учетной записи осуществляется контроль соответствия параметров установленного пароля требованиям РД.	Осуществляется средствами ОС СН. Решение задачи идентификации и аутентификации пользователей в ОС основывается на использовании механизма PAM, который представляет собой набор разделяемых библиотек (модулей), с помощью которых администратор может организовать процедуру аутентификации (подтверждение подлинности) пользователей прикладными программами. Каждый модуль реализует собственный механизм аутентификации. Изменяя набор и порядок следования модулей, можно построить сценарий аутентификации. Подобный подход позволяет изменять процедуру аутентификации без изменения исходного кода и повторного компилирования PAM. Сценарии аутентификации описываются в конфигурационных файлах. Если ОС не настроена для работы в ЕПП, то аутентификация осуществляется с помощью локальной БД пользователей. При использовании ЕПП аутентификация пользователей осуществляется централизованно по протоколу Kerberos. Решение задачи организации ЕПП (создание домена) обеспечивает:

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			Производятся следующие действия: попытка входа в АС с использованием некорректного идентификатора; попытка входа в АС с использованием корректного идентификатора и неверного пароля; попытка входа в АС с использованием некорректного идентификатора и корректного пароля. Если хотя бы у одной учетной записи количество попыток входа с неверными реквизитами превышает установленное максимальное число неудачных попыток входа пользователей в АС, должна осуществляется блокировка работы пользователя. В случае если пользователи автоматизированной системы имеют возможность изменять собственные пароли, под учетными записями пользователей производятся попытки установить пароль, не соответствующий требованиям РД. Осуществляются: попытка установить пароль, длина которого менее 8 символов; попытки установить пароль, состоящий исключительно из цифр, либо только из букв.	-сквозную аутентификацию в сети; -централизацию хранения информации об окружении пользователей; -централизованную настройку правил регистрации событий безопасности в рамках домена; -централизованный учет и идентификацию подключаемых устройств. Сетевая аутентификация и централизация хранения информации об окружении пользователя подразумевает использование двух основных механизмов: NSS и PAM. В среде ОС СН пользователю поставлен в соответствие ряд атрибутов, характеризующих его мандатные права. Концепция ЕПП подразумевает хранение системной информации о пользователе (включая доступные мандатные уровни и категории) централизованно. В данном случае вся информация хранится в службе каталогов LDAP. Администратор сети может централизованно управлять конфигурацией сети, разграничивать доступ к сетевым сервисам. Для управления пользователями, группами и настройками их атрибутов используется графическая утилита, соотвествующие настройки обеспечивают требования к длине пароля.
1.2	Идентификация терминалов, ЭВМ, узлов сети ЭВМ,	Проверка возможностей системы защиты АС по идентификации	Для проверки идентификации узлов сети ЭВМ осуществляются следующие действия:	Осуществляется средствами ОС СН. Идентификация терминалов — по

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
	каналов связи, внешних устройств ЭВМ по физическим адресам (номерам)	терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по физическим адресам (номерам)	контроль наличия уникальных физических адресов у всех узлов сети путем применения штатных средств операционных систем объекта испытаний; осуществляются попытки передачи контрольной информации между несколькими узлами сети (для передачи информации с узла-отправителя на узел-получатель в ходе проверок должен использоваться физический адрес узла получателя).	номеру терминала, ЭВМ — по MAC-дресу, узлы сети — по IP-адресу, внешние устройства — по именам соответствующих файлов в /dev
1.3	Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам	Проверка возможностей системы защиты АС по идентификации программ, томов, каталогов, файлов, записей, полей записей по именам	Проверка функциональных возможностей ОО по идентификации программ, каталогов, файлов и других ресурсов. Для проверки возможностей системы защиты АС по идентификации программ необходимо выполнить следующие действия: запустить приложение "Терминал"; назначить пользователям разные права на запуск для одной из программ из состава АС; осуществить тестовые попытки запуска программы под учетными записями пользователей	Осуществляется средствами ОС СН и СУБД из состава ОС СН. Идентификация осуществляется по логическим именам томов, каталогов, файлов, записей, полей записей.
1.4	Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа	Проверка возможностей системы защиты АС по осуществлению контроля доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа	Выбирается несколько учетных записей пользователей и несколько защищаемых ресурсов. В выборку должны быть включены пользователи с различными правами доступа к выбранным ресурсам, права доступа некоторых пользователей к ресурсам должны быть ограниченными (например, только чтение и т. д.). Далее для каждой выбранной учетной записи с использованием штатных программных средств объекта испытаний осуществляются попытки санкционированного и несанкционированного доступа	Осуществляется средствами ОС СН и СУБД из состава ОС СН. При этом принятие решения о запрете или разрешении доступа субъекта к объекту принимается на основе типа запрашиваемого субъектом доступа и правил дискреционнного разграничения доступа заданных для каждого объекта.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			пользователей к выбранным ресурсам. Примерами попыток несанкционированного доступа могут быть следующие действия: попытка чтения пользователем объекта (файл, каталог, устройство), если у пользователя отсутствуют какие-либо права на доступ к данному объекту; попытка записи пользователем в объект (файл, каталог, устройство), если у пользователя отсутствуют права на запись в данный объект; попытка удаления пользователем объекта (файл, каталог, устройство), если у пользователя отсутствуют права на удаление данного объекта.	
1.5	Управление потоками информации с помощью меток конфиденциальности	Проверка возможностей системы защиты АС по управлению потоками информации с помощью меток конфиденциальности. При этом уровень конфиденциальности накопителей должен быть не ниже уровня конфиденциальности, записываемой на них информации	Для проверки возможности управления потоками информации с помощью меток конфиденциальности осуществляются следующие действия: произвольным образом выбирается несколько учетных записей пользователей и несколько защищаемых ресурсов с различными метками конфиденциальности. Далее для каждой выбранной учетной записи с использованием штатных программных средств объекта испытаний (менеджер файлов из состава ОО) осуществляются следующие действия; вход в АС под "несекретной" учетной записью; попытки чтения объектов и записи в объекты, уровень конфиденциальности которых не выше чем текущий уровень конфиденциальности пользователя; попытки чтения объектов, уровень конфиденциальности которых выше уровня конфиденциальности текущего пользователя;	Осуществляется средствами ОС СН и СУБД из состава ОС СН. Управление потоками осуществляется на основе меток конфиденциальности пользователей с применением мандатной политики ОС СН и СУБД из состава ОС СН. Управление потоками информации при доступе субъекта к объекту осуществляется на основе мандатного контекста безопасности субъекта и мандатной метки объекта. Контроль доступа осуществляется путем задания соответствующих прав.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			вход в АС под "секретной" учетной записью пользователя; попытки чтения объектов с различными уровнями конфиденциальности; попытки записи в объекты, уровень конфиденциальности которых равен текущему уровню допуска пользователя к защищаемым ресурсам АС; попытки записи в объекты, уровень конфиденциальности которых ниже текущего уровня допуска пользователя к защищаемым ресурсам АС.	
2	Подсистема регистрации и учета:			В ОС СН реализована расширенная подсистема протоколирования, осуществляющая регистрацию событий в двоичные файлы.
2.1	Регистрация входа (выхода) субъектов доступа в систему (из системы)	Проверка возможностей системы защиты АС по регистрации входа (выхода) субъектов доступа в АС (из АС), либо регистрации загрузки и инициализации ОС и ее программного останова. Регистрация выхода из автоматизированной системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются: дата и время входа (выхода) субъекта доступа (должностного лица) в АС (из АС) или загрузки (останова) АС; результат попытки входа: успешная или неуспешная - несанкционированная;	В ходе проверки осуществляется контроль корректности произведенной настройки ОО, касающейся регистрации событий входа (выхода) субъектов доступа в АС (из АС) с использованием средств администрирования. Далее произвольным образом выбирается несколько учетных записей пользователей. Для каждой выбранной учетной записи производятся следующие действия: попытки входа пользователей в автоматизированную систему с некорректными учетными данными (идентификатор, пароль); попытки входа пользователей в АС с корректными учетными данными (идентификатор, пароль); выход пользователей из автоматизированной	Осуществляется средствами ОС СН. Регистрация входа/выхода пользователей ОС СН осуществляется в журнале. В параметрах регистрации указываются: дата и время события, результат попытки входа, идентификатор пользователя, код при неуспешной попытке. В качестве кода подразумевается имя пользователя UID. Регистрация загрузки операционной системы осуществляется средствами СДЗ.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
		идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа; код или пароль, предъявленный при неуспешной попытке	системы. В случае необходимости осуществляется программный останов ОС и ее последующая загрузка. Затем осуществляется анализ журналов с целью определения степени полноты регистрации всех рассматриваемых в данном пункте событий и наличия необходимых параметров регистрации.	
2.2	Регистрация выдачи печатных (графических) документов на "твердую" копию	Проверка возможностей системы защиты АС по регистрации выдачи печатных (графических) документов на "твердую" копию.	Выдача сопровождается 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;	Осуществляется средствами ОС СН. Управление заданиями на печать и маркировкой документов осуществляется с помощью веб-приложения «управление печатью» из состава ОС СН. Маркировка отпечатанных листов документа осуществляется при соответствующей настройке защищенного комплекса программ печати и маркировки документов из состава ОС СН.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			идентификатор субъекта доступа, запросившего документ; объем фактически выданного документа (количество страниц, листов, копий) и результат выдачи успешный (весь объем), неуспешный.	
2.3	Регистрация запуска (завершения) всех программ и процессов (заданий, задач в АС	Проверка возможностей системы защиты АС по регистрации запуска (завершения) всех программ и процессов (заданий, задач) в АС.	В ходе данной проверки осуществляется контроль корректности произведенной настройки, касающейся регистрации запуска (завершения) программ и процессов, предназначенных для обработки защищаемых файлов, с использованием штатных средств администрирования. Кроме этого оценивается полнота регистрируемой информации. Для проверки возможностей системы защиты АС по регистрации запуска программ и процессов необходимо выполнить следующие действия: последовательна авторизация на под учетными записями пользователей, обладающих различными правами на запуск одной из программ из состава изделия; осуществление попыток запуска программы (как санкционированные, так и несанкционированные); провести анализ журналов с целью определения степени полноты регистрации всех рассматриваемых в данном пункте событий и наличия всех необходимых параметров регистрации.	Осуществляется средствами ОС СН. Настройка регистрации событий для пользователей (аудит процессов) осуществляется с помощью локальной и доменной политики безопасности (аудит события «exec») fly-admin-smc. Настройка аудита событий осуществляется утилитой setfaud. Просмотр регистрируемых событий осуществляется через журналах безопасности. В параметрах регистрации указываются дата и время запуска, наименование запускаемой программы, логин пользователя, статус запуска.
2.4	Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к	Проверка возможностей системы защиты АС по регистрации попыток доступа программных средств (программ, процессов, задач, заданий)	Осуществляется проверка установленных в АС параметров регистрации (режимов регистрации операций чтения, записи, удаления, изменения разрешений, изменения	Осуществляется средствами ОС СН. Настройка регистрации осуществляется с помощью локальной и доменной политики безопасности. Настройка

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
	защищаемым файлам	к защищаемым файлам.	владельцев), контроль установленных параметров аудита, касающихся регистрации попыток доступа программных средств к защищаемым файлам. Параметры регистрации файловых операций определяются с использованием средства администрирования АПК. Для тестовых учетных записей осуществить следующие действия: войти в автоматизированную систему под "несекретной" учетной записью; с использованием штатных программных средств объекта испытаний (менеджер файлов из состава ОС СН) выполнить следующие операции над защищаемыми файлами: чтение, запись, удаление, создание файлов, уровень конфиденциальности которых равен текущему уровню конфиденциальности пользователя, попытки чтения файлов, уровень конфиденциальности которых выше текущего уровня конфиденциальности пользователя; войти в автоматизированную систему под "секретной" учетной записью; с использованием штатных программных средств объекта испытаний (менеджер файлов из состава ОС СН) выполнить следующие операции над защищаемыми файлами: чтение, запись, удаление, создание файлов, уровень конфиденциальности которых равен текущему уровню конфиденциальности пользователя, попытки записи, чтения файлов, уровень конфиденциальности которых ниже текущего уровня конфиденциальности пользователя; провести анализ журналов с целью определения степени полноты регистрации всех рассматриваемых в данном пункте	аудита событий осуществляется утилитой. Просмотр регистрируемых событий осуществляется через журнал безопасности. В параметрах регистрации указываются дата и время запуска, наименование запускаемой программы, логин пользователя, статус запуска.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			событий и наличия всех необходимых параметров регистрации.	
2.5	Регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа	Проверка возможностей системы защиты АС по регистрации 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	Осуществляется проверка установленных в АС параметров регистрации (режимов регистрации операций чтения, записи, удаления, изменения разрешений, изменения владельцев), контроль установленных свойств аудита, касающихся регистрации попыток доступа программных средств к защищаемым объектам доступа. Для тестовых учетных записей осуществить следующие действия: войти в АС под "несекретной" учетной записью; с использованием штатных программных средств объекта испытаний (менеджер файлов из состава СО СН) выполнить следующие операции над защищаемыми объектами: чтение, запись, удаление, создание файлов, уровень конфиденциальности которых равен текущему уровню конфиденциальности пользователя, попытки чтения файлов, уровень конфиденциальности которых выше текущего уровня конфиденциальности пользователя; открытие, создание, удаление каталогов с равным уровнем конфиденциальности, попытки открытия каталогов с более высоким уровнем конфиденциальности; попытки чтения (открытия) томов с равным и более высоким уровнем конфиденциальности (если такие есть); формирование и выполнение информационных запросов к базам данных объекта испытаний; ввод\вывод защищаемой информации с равным уровнем конфиденциальности на внешние носители; печать документа на одном из печатающих устройств объекта испытаний; доступ к ЭВМ,	Осуществляется средствами ОС СН. Настройка регистрации осуществляется с помощью локальной и доменной политики безопасности. Просмотр регистрируемых событий осуществляется через журналы безопасности. В параметрах регистрации указываются дата и время попытки доступа, идентификатор субъекта доступа, спецификация защищаемого объекта, имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту, вид запрашиваемой операции. Регистрация доступа к терминалам и ЭВМ может осуществляться средствами СДЗ.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			узлам сети ЭВМ, каналам связи и терминалам; войти в автоматизированную систему под "секретной" учетной записью; с использованием штатных программных средств объекта испытаний (менеджер файлов из состава ОС СН) выполнить следующие операции над защищаемыми файлами: чтение, запись, удаление, создание файлов, уровень конфиденциальности которых равен текущему уровню конфиденциальности пользователя, попытки записи, чтения файлов, уровень конфиденциальности которых ниже текущего уровня конфиденциальности пользователя; открытие, создание, удаление каталогов с равным уровнем конфиденциальности, попытки записи файлов в каталоги, открытие каталогов с более низким уровнем конфиденциальности; попытки чтения (открытия) томов с равным и более низким уровнем конфиденциальности (если такие есть); формирование и выполнение информационных запросов к базам данных объекта испытаний; ввод\вывод защищаемой информации с равным уровнем конфиденциальности на внешние носители; печать документа на одном из печатающих устройств объекта испытаний; доступ к ЭВМ, узлам сети ЭВМ, каналам связи и терминалам; провести анализ журналов с целью определения степени полноты регистрации всех рассматриваемых в данном пункте событий и наличия всех необходимых параметров регистрации.	
2.6	Регистрация изменений полномочий субъектов доступа и статуса объектов доступа	Проверка возможностей системы защиты АС по регистрации изменений полномочий субъектов доступа и статуса объектов доступа	Осуществляется проверка установленных в АС параметров регистрации и контроль установленных свойств аудита, касающихся регистрации изменений полномочий субъектов	Осуществляется средствами ОС СН. Настройка регистрации осуществляется с помощью локальной и доменной политики безопасности Просмотр

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			доступа и статуса объектов доступа. Для проверки возможностей системы защиты АС по регистрации изменений полномочий субъектов доступа и статуса объектов доступа необходимо выполнить следующие действия: под учетной записью администратора информационной безопасности АС изменить уровень допуска (секретности) нескольких пользователей (изменение полномочий субъектов доступа); под учетной записью администратора информационной безопасности АС изменить уровень конфиденциальности (секретности) нескольких защищаемых ресурсов (изменение статуса объектов доступа); под учетной записью администратора информационной безопасности АС изменить права доступа нескольких пользователей к каким-либо защищаемым ресурсам АС (изменение полномочий субъектов доступа и статуса объектов доступа; провести анализ журналов ОО с целью определения степени полноты регистрации всех рассматриваемых в данном пункте событий и наличия всех необходимых параметров регистрации.	регистрируемых событий осуществляется через журналы безопасности. 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, спецификация объекта, у которого проведено изменение статуса зашиты и вид изменения.
2.7	Автоматический учет создаваемых защищаемых файлов	Проверка возможностей системы защиты АС по автоматическому учету 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	Для проверки корректности функционирования подсистемы автоматического учета произвольным образом выбирается несколько учетных записей пользователей АС. Для каждой выбранной учетной записи производятся следующие действия: вход в автоматизированную систему с одним из доступных уровней конфиденциальности;	Осуществляется средствами ОС СН , средствами мандатной политики. При создании субъектом любого из следующих объектов механизмы многопроцессорного взаимодействия, стек TCP/IP (IPv4), ФС Ext2/Ext3/Ext4, сетевые ФС CIFS, ФС proc, tmpfs, объект наследует метку на основе мандатного контекста безопасности процесса. С

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
		дополнительной маркировки, используемой в подсистеме управления доступом. Маркировка должна отражать уровень конфиденциальности объекта	создание в защищаемых каталогах объекта испытаний тестовых файлов; копирование защищаемых файлов с различным уровнем конфиденциальности в защищаемые каталоги; подключение и регистрация внешнего устройства; Далее необходимо определить уровни конфиденциальности созданных\скопированных тестовых файлов. Убедиться в автоматическом запросе назначения уровня конфиденциальности при регистрации нового внешнего устройства.	каждым субъектом и объектом связаны мандатный контекст безопасности и мандатная метка соотвественно. ОС СН обеспечивает ввод-вывод информации на запрошенное пользователем устройство.
2.8	Учет всех защищаемых носителей информации	Проверка возможностей системы защиты АС по учету всех защищаемых носителей информации с помощью их маркировки и занесением учётных данных в журнал (учетную карточку)	На данном этапе осуществляется проверка документации на предмет наличия в ней описаний процедур, позволяющих реализовать учет и маркировку защищаемых носителей информации на объекте испытаний.	Осуществляется средствами ОС СН и организационными мерами. В ОС СН учет защищаемых носителей информации может осуществляться в локальной базе данных или ЕПП. Регистрация осуществляется в специальных журналах учета
2.9	Учет защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема)	Проверка возможностей системы защиты АС по учету защищаемых носителей в журнале (картотеке) с регистрацией их выдачи (приема)	Осуществляется проверка реализованных на объекте эксплуатации организационных мер, позволяющих выполнить в данной АС требования РД учету защищаемых носителей информации в журналах с регистрацией их выдачи (приема). В ходе проверки проводится анализ документации на предмет наличия в ней описаний процедур, позволяющих вести учет защищаемых носителей информации в журналах с регистрацией их выдачи (приема) на объекте испытаний.	Организационными мерами. Регистрация осуществляется в специальных журналах учета
2.10	Проведение нескольких видов учёта (дублирующих)	Проверка возможностей системы защиты АС по проведению	Осуществляется проверка наличия в АС нескольких видов учета защищаемых	Осуществляется средствами ОС СН и организационными мерами.

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
	защищаемых носителей информации	нескольких видов учёта (дублирующих) защищаемых носителей информации	носителей информации. Проводится анализ документации на предмет наличия в ней описаний процедур, позволяющих реализовать несколько видов учета защищаемых носителей информации на объекте испытаний. Далее проверяется реализация данных видов учета в АС (проверка наличия журналов и т.д).	
2.11	Очистка (обнуление, обезличивание) освобождаемых областей памяти	Проверка возможностей системы защиты АС по очистке (обнулению, обезличиванию) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется двукратной произвольной записью в любую освобождаемую область памяти, ранее использованную для хранения защищаемой информации	В ходе данной проверки проводится оценка соответствия проведенных настроек, касающихся функционирования очистки памяти на объекте испытаний, требованиям РД. На начальном этапе определяется наличие и особенности применения штатных средств очистки памяти объекта испытаний (очистка может производиться автоматически при удалении информации из памяти или только после применения специализированных программных средств и т. д.). Так же проводится оценка корректности настроек штатных средств очистки памяти объекта испытаний. Механизмы очистки памяти должны быть доступны (активны) на всех этапах технологического процесса обработки информации в АС и количество циклов обнуления (обезличивания) освобождаемых областей памяти, установленное в ходе проведенных администратором настроек, должно быть не менее двух.	Осуществляется средствами СО СН. Ядро ОС СН гарантирует, что обычный непривелигированный процесс не получит данные чужого рпоцесса, если это явно не разрешено ПРД. Средства межпроцессорного взаимодействия котнролируются с помощю ПРД, и процесс не может получить неочищенную память (оперативную и дисковую). Также в ОС СН реализован механизм, который очищает неиспользуемые блоки файловой системы непосредственно при их освобождении. Работа данного механизама снижает скорость выполнения операций удаления и усечения размера файла. Данные любях файлов в пределах заданной ФС предварительно очищаются предопределенной или псевдослучайной маскирующей последовательностью.
2.12	Сигнализация попыток НСД	Проверка возможностей системы защиты АС по сигнализации попыток НСД	Для проверки возможностей системы защиты АС по сигнализации попыток нарушения защиты необходимо выполнить следующие действия: под учетными записями пользователей осуществить попытки входа в АС с использованием некорректного идентификатора;	Для решения задач централизованного протоколирования и анализа журналов аудита, а также организации распределенного мониторинга сети, жизнеспособности и целостности серверов используется программное решение Zabbix. Zabbix предоставляет гибкий механизм

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			под учетными записями пользователей осуществить попытки входа в АС с использованием корректного идентификатора и неверного пароля; под учетными записями пользователей осуществить попытки входа в АС с использованием корректного и некорректного идентификатора; под учетными записями пользователей осуществить попытки доступа к защищаемым ресурсам АС в обход установленных правил дискреционного разграничения доступа; под учетными записями пользователей осуществить попытки доступа к защищаемым ресурсам АС в обход установленных правил мандатного разграничения доступа; под учетными записями пользователей осуществить нарушение целостности файлов; под учетными записями пользователей осуществить запуск неразрешенных программ. В ходе осуществления указанных выше действий необходимо фиксировать реакцию ОО. В результате анализа должны быть получены следующие сведения о параметрах функционирования: способы сигнализации о попытках НСД, реализованные на рабочих местах пользователей и рабочем месте администратора информационной безопасности; условия срабатывания сигнализации о попытках НСД; информация, которую может получить	сбора данных. Все отчеты и статистика Zabbix, а также параметры настройки компонентов Zabbix доступны через web-интерфейс. В web-интерфейсе реализован следующий функционал: - вывод отчетности и визуализация собранных данных; - создание правил и шаблонов мониторинга состояния сети и узлов; - определение допустимых границ значений заданных параметров; - настройка оповещений; - настройка автоматического реагирования на события безопасности

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			администратор информационной безопасности из сообщений о попытках нарушения защиты.	
3	Криптографическая подсистема	Обеспечивается средствами криптографической защиты информации		
4	Подсистема обеспечения целостности			
4.1	Обеспечение целостности программных средств СЗИ от НСД, а также целостность программной среды	Проверка возможностей системы защиты АС по обеспечению целостности программных средств ОО, а также неизменности программной среды. При этом: целостность ОО 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.	В ходе данной проверки необходимо осуществить следующие действия. с использование средств администрирования определить список файлов, целостность которых контролируется; определить условия, при которых производится проверка целостности (при загрузке АС, по требованию пользователя, при входе пользователя и т. д.); определить способ проверки целостности исполняемых файлов (по контрольным суммам, по наличию имен исполняемых файлов и т. д.); определить реакцию АС на нарушение целостности исполняемых файлов (сигнализация, блокировка рабочей станции, регистрация в журналах и т. д.); создать копию одного из исполняемых файлов; внести созданную копию в список файлов, целостность которых контролируется в АС; переименовать созданную копию и изменить ее содержимое; перезагрузить рабочую станцию и в случае необходимости осуществить вход в АС под учетной записью пользователя, зарегистрированного на выбранной рабочей станции;	Осуществляется встроенными СЗИ ОС СН. Для решения задач контроля целостности предназначена библиотека libgost, в которой для вычисления контрольных сумм реализованы функции хэширования в соответствии с ГОСТ Р 34.11-94, ГОСТ Р 34.11-2012 с длиной хэш-кода 256 бит и ГОСТ Р 34.11-2012 с длиной хэш-кода 512 бит. Названная библиотека используется в средствах подсчета контрольных сумм файлов и оптических дисков, контроля соответствия дистрибутиву и регламентного контроля целостности, модулях аутентификации и средствах контроля целостности ФС. Контроль целостности дистрибутива обеспечивается методом расчета его контрольных сумм файлов, установленных в системе, и сравнения полученного значения с эталонными значениями контрольных сумм. Контроль целостности исполняемых файлов и библиотек формата ELF ОС СН (в том числе СЗИ) и прикладного ПО модулем ядра digsig_verify с использованием функции хэширования в соотвествии с ГОСТ Р 34.11-94 и ЭЦП, реализованной в соотвествии с ГОСТ Р 34.10-2001, динамически непосредственно при их отображении в

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
			проанализировать реакцию АС на произведенные изменения целостности программной среды.	адресное пространство процесса. Регламентный контроль целостности обеспечивается набором программных средств, который представляет возможность периодического (с использованием системного планировщика заданий cron) вычисления контрольных сумм файлов и соответствующих им атрибутов с последующим сравнением вычисленных значений с эталонными. В указанном наборе программных средств реализовано использование библиотеки libgost и контроль целостности связанных с файлами атрибутов расширенной подсистемы безопасности PARSEC (мандатных атрибутов и атрибутов расширенной подсистемы протоколирования). Целостность загрузчика и ядра ОС СН обеспечивается средствами СДЗ. Применение антивирусных средств обеспечивает защиту от разрушающих программных воздействий.
4.2	Физическая охрана СВТ	Проверка реализации в АС физической охраны СВТ	В ходе данной проверки осуществляется контроль наличия постоянной физической охраны территории, здания и помещений, где располагается объект испытаний, с помощью технических средств охраны и специального персонала, а также наличие строгого пропускного режима и специально оборудованных помещений в соответствии с действующими нормативными документами. Проводится анализ документации на предмет наличия в ней требований к физической охране СВТ из состава АС.	Осуществляется организационно-техническими мерами, отраженными в эксплуатационной документации

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
4.3	Наличие администратора (службы) защиты информации	Проверка наличия администратора (службы) защиты информации, ответственного за ведение, нормальное функционирование и контроль работы СЗИ от НСД. Администратор должен иметь свой терминал и необходимые средства оперативного контроля и воздействия на безопасность АС	Необходимо выполнить следующие действия: проверить наличие администратора информационной безопасности в изделии; провести анализ документации АС с целью контроля наличия в ней сведений, регламентирующих деятельность администратора информационной безопасности изделия (руководство администратора информационной безопасности и т. д.); проверить наличие выделенного автоматизированного рабочего места и специализированных средств контроля и управления информационной безопасностью.	Осуществляется организационными мерами и средствами ОС СН. В ОС СН существует возможность организовать единое пространство пользователей (ЕПП), которое представляет собой средства организации работы пользователя в сети АРМ, работающих под управлением ОС СН. Организация ЕПП обеспечивает сквозную организацию в сети, централизацию хранения информации об окружении пользователей, централизацию хранения настроек системы защиты информации на сервере. Средства организации ЕПП включают в себя средства администрирования. Решение задачи оперативного контроля обеспечивается средствами централизованного сбора и анализа журналов протоколирования (журналов аудита) в ОС СН.
4.4	Периодическое тестирование функций СЗИ от НСД	Проверка реализации в АС периодического тестирования всех функций СЗИ от НСД с помощью специальных программных средств, имитирующих попытки НСД	В ходе данной проверки необходимо осуществить следующие действия. проверить в документации на АС наличие и полноту сведений о порядке проведения тестирования (периодичность, использование инструментальных средств и т. д.); проверить наличие специальных программных средств для проведения периодического тестирования всех функций.	Осуществляется встроенными средствами тестирования СЗИ СО СН и СДЗ. В состав ОС СН входят средства тестирования функций СЗИ от НСД, находящиеся в каталоге *usr*lib/parsec/tests. Данный набор обеспечивает тестирование всех функций СЗИ от НСД из состава ОС СН, включая: управление доступом, регистрация событий, очистка памяти, изоляция модулей, идентификация и аутентификация. В состав ОС СН входят средства

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
				тестирования функций СЗИ СУБД, обеспечивающие тестирование всех функций СЗИ СУБД, включая управление доступом, регистрацию событий, идентификацию и аутентификацию.
4 .5	Наличие средств восстановления СЗИ от НСД	Проверка наличия средств восстановления СЗИ от НСД, предусматривающих ведение двух копий программных средств СЗИ от НСД и их периодическое обновление и контроль работоспособности, а также оперативное восстановление функций СЗИ от НСД при сбоях	В ходе данной проверки необходимо осуществить следующие действия: проверить в документации на АС наличие и полноту сведений о порядке проведения процедуры восстановления всех функций СЗИ от НСД; проверить наличие средств восстановления работоспособности системы (дистрибутивы ОПО, СПО, ПО СЗИ от НСД, резервные копии программных средств СЗИ от НСД), ведение двух копий программных средств СЗИ от НСД.	Осуществляется организационными мерами и средствами ОС СН. Средства организации ЕПП ОС СН предоставляют возможность развертывания основного и резервных серверов ALD, обеспечивающих ведение двух или более программных средств СЗИ НСД и баз данных безопасности. В ОС СН существует возможность в процессе загрузки после сбоя автоматически выполнять программу проверки и восстановления ФС - fsck. Если повреждения ФС окажутся незначительными, то ее выполнения достаточно для обеспечения целостности ФС. В случае обнаружения серьезных повреждений ФС данная программа предлагает перезагрузить компьютер в однопользовательский режим и провести запуск программы вручную. Администратор, контролирующий процесс загрузки ОС СН, после сбоя должен следовать инструкциям, выдаваемым программой fsck. После завершения загрузки ОС СН следует проверить целостность файлов с помощью программы контроля целостности. Если сбой привел к выводу из строя жестких дисков, следует заменить

№ п/п	Требования РД АС	Цель проверки	Способ проверки	Предложения по реализации
				вышедшее из строя оборудования и переустановить ОС СН с диска с дистрибутивом, а пользовательские данные восстановить с резервной копии. В состав ОС СН входят средства (комплекс программ Bacula, утилиты rsync и tar0 для выполнения операций резервного копирования и восстановления объектов ФС с сохранением и восстановлением мандатных атрибутов и атрибутов аудита. Резервное копирование используется для восстановления файлов, случайно удаленных пользователями или утерянных из-за отказов устройств хранения, получения периодически создаваемых снимков состояния данных, получения данных для восстановления после аварий.
4.6	Использование сертифицированных средств защиты	Проверка наличия действующих сертификатов на используемые средства защиты информации от несанкционированного доступа	В ходе данной проверки необходимо осуществить проверку наличия действующих сертификатов на используемые в АС средства защиты информации от несанкционированного доступа	Выполняется при условии применения сертифицированных СЗИ, подходящих под класс «1Б», а также сертификации всего программного обеспечения.