Инструкция по проверке действия функций средства защиты информации Secret Net 7

Данный документ содержит общий перечень действий для тестирования функций разграничения доступа к информации, обрабатываемой с использованием средства защиты информации Secret Net 7. Конкретный список действий, которые подлежат выполнению при периодическом тестировании системы, формируется на основе общего перечня исходя из требований политики безопасности в организации, используемых защитных механизмов и вариантов применения СЗИ Secret Net.

Тестирование функции считается завершенным успешно, если полученный результат совпадает с ожидаемым.

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
Проверка отсутствия ошибок функционального контроля подсистем СЗИ на компьютере			
Перезагрузить компьютер, войти в систему и загрузить для просмотра журнал Secret Net	Загрузка журнала осуществляется. В журнале отсутствует событие "Ошибка выполнения функционального контроля" (тип "Аудит отказов")		
Проверка контроля входа пользователей в систему			
Если в групповой политике включен режим "Вход в систему: Разрешить интерактивный вход только доменным пользователям" — выполнить попытку входа в систему с вводом учетных данных локального пользователя	Отказ во входе в систему с выдачей сообщения о запрете входа локальным пользователям		
Если в групповой политике включен режим "Стандартная аутентификация" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "По имени" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом неправильного пароля пользователя	Отказ во входе в систему с выдачей сообщения о неверном пароле или имени пользователя. Если в ОС Windows включена регистрация событий входа/выхода, имеющих тип "Аудит отказов", то в журнале безопасности будет событие отказа входа в систему для пользователя с неправильным паролем		
• с вводом правильного имени и пароля пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
Если в групповой политике включен режим "Стандартная аутентификация" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "Смешанный" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом неправильного пароля пользователя	Отказ во входе в систему с выдачей сообщения о неверном пароле или имени пользователя. Если в ОС Windows включена регистрация событий входа/выхода, имеющих тип "Аудит отказов", то в журнале безопасности будет событие отказа входа в систему для пользователя с неправильным паролем		
• с предъявлением персонального идентификатора, не зарегистрированного в системе	Отказ во входе в систему с выдачей сообщения "Предъявленный идентификатор не присвоен ни одному пользователю". В журнале Secret Net регистрируется событие "Идентификатор не зарегистрирован" (тип "Аудит отказов") категории "Вход/выход"		
• с вводом правильного имени и пароля пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
• с предъявлением персонального идентификатора пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
Если в групповой политике включен режим "Стандартная аутентификация" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "Только по идентификатору" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом имени и пароля пользователя с клавиатуры	Отказ во входе в систему с выдачей сообщения "Вход без электронного идентификатора запрещен"		
• с предъявлением персонального идентификатора, не зарегистрированного в системе	Отказ во входе в систему с выдачей сообщения "Предъявленный идентификатор не присвоен ни одному пользователю". В журнале Secret Net регистрируется событие "Идентификатор не зарегистрирован" (тип "Аудит отказов") категории "Вход/выход"		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
• с предъявлением персонального идентификатора пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
Если в групповой политике включен режим "Усиленная аутентификация по ключу" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "По имени" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом неправильного пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом пользователя	Отказ во входе в систему с выдачей сообщения о неверном пароле или имени пользователя. Если в ОС Windows включена регистрация событий входа/выхода, имеющих тип "Аудит отказов", то в журнале безопасности будет событие отказа входа в систему для пользователя с неправильным паролем		
• с вводом правильного имени и пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом другого пользователя	Отказ во входе в систему с выдачей сообщения "предъявленные аутентификационные данные не принадлежат заявленному пользователю". В журнале Secret Net регистрируется событие "Запрет входа пользователя" (тип "Аудит отказов") с указанием причины запрета — не предъявлен ключ		
• с вводом правильного имени и пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
Если в групповой политике включен режим "Усиленная аутентификация по ключу" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "Смешанный" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом неправильного пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом пользователя	Отказ во входе в систему с выдачей сообщения о неверном пароле или имени пользователя. Если в ОС Windows включена регистрация событий входа/выхода, имеющих тип "Аудит отказов", то в журнале безопасности будет событие отказа входа в систему для пользователя с неправильным паролем		
• с вводом правильного имени и пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом другого пользователя	Отказ во входе в систему с выдачей сообщения "предъявленные аутентификационные данные не принадлежат заявленному пользователю". В журнале Secret Net регистрируется событие "Запрет входа пользователя" (тип "Аудит отказов") с указанием причины запрета — не предъявлен ключ		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
• с предъявлением персонального идентификатора, не зарегистрированного в системе	Отказ во входе в систему с выдачей сообщения "Предъявленный идентификатор не присвоен ни одному пользователю". В журнале Secret Net регистрируется событие "Идентификатор не зарегистрирован" (тип "Аудит отказов") категории "Вход/выход"		
• с вводом правильного имени и пароля пользователя и далее по запросу системы предъявить идентификатор с закрытым ключом пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
• с предъявлением персонального идентификатора пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
Если в групповой политике включен режим "Усиленная аутентификация по ключу" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "Только по идентификатору" для параметра "Вход в систему: Режим идентификации пользователя" — выполнить попытки входа пользователя в систему:			
• с вводом имени и пароля пользователя с клавиатуры	Отказ во входе в систему с выдачей сообщения "Вход без электронного идентификатора запрещен"		
• с предъявлением персонального идентификатора, не зарегистрированного в системе	Отказ во входе в систему с выдачей сообщения "Предъявленный идентификатор не присвоен ни одному пользователю". В журнале Secret Net регистрируется событие "Идентификатор не зарегистрирован" (тип "Аудит отказов") категории "Вход/выход"		
• с предъявлением персонального идентификатора пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		
Если в групповой политике включен режим "Усиленная аутентификация по паролю" для параметра "Вход в систему: Режим аутентификации пользователя" и режим "Смешанный" для параметра "Вход в систему: Режим идентификации пользователя" — разрешить пользователю разовый вход для сохранения пароля (в параметрах пользователя установить отметку в поле "Доверять парольной аутентификации Windows при следующем входе в систему") и выполнить попытку входа в систему с вводом правильного имени и пароля пользователя	Вход в систему разрешается. В журнале Secret Net регистрируется событие "Вход пользователя в систему" (тип "Аудит успехов") с указанием режимов работы подсистемы		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
Проверка контроля целостности защищаемых ресурсов			
Если на компьютере настроен механизм контроля целостности — выполнить следующие действия:			
• войти в систему с учетными данными администратора и загрузить для просмотра журнал Secret Net	В журнале Secret Net регистрируются события "Начало обработки задания на контроль целостности" и "Успешное завершение задания на контроль целостности" (тип "Аудит успехов")		
• в программе "Контроль программ и данных" создать контролируемый ресурс (например, каталог, содержащий несколько текстовых файлов). Сформировать для данного ресурса задание на контроль содержимого файлов по алгоритму "Имитовставка". В расписании выполнения данного задания указать, что контроль выполняется после входа. Настроить регистрацию нарушения контроля целостности, в качестве реакции системы выбрать блокировку компьютера. Рассчитать эталоны контролируемых параметров. Произвести изменение содержимого файлов в каталоге, поставленном на контроль. Войти в систему с учетными данными рядового пользователя	При входе пользователя срабатывает контроль целостности и компьютер блокируется. При попытке разблокировать компьютер пользователю выдается сообщение о необходимости обратиться к администратору		
• разблокировать компьютер с использованием учетных данных администратора и загрузить для просмотра журнал Secret Net	В журнале Secret Net регистрируются события "Нарушение целостности ресурса" и "Компьютер заблокирован системой защиты" (тип "Аудит отказов")		
• в программе "Контроль программ и данных" удалить тестовое задание и сохранить базу. Войти в систему с учетными данными рядового пользователя	Компьютер не блокируется, нарушений контроля целостности не регистрируется		
Если на компьютере настроен механизм контроля целостности и включен режим совместной работы СЗИ Secret Net с ПАК "Соболь" — выполнить следующие действия:			
• перезагрузить компьютер, войти в ПАК "Соболь" с использованием идентификатора пользователя	Вход в ПАК "Соболь" выполняется успешно, отсутствуют ошибки при проверке целостности ресурсов средствами ПАК		
• войти в систему, изменить тестовый ресурс, который присутствует в задании на контроль целостности ПАК "Соболь". Перезагрузить компьютер и войти в ПАК "Соболь" с использованием идентификатора пользователя	При входе пользователя в ПАК "Соболь" фиксируется ошибка контроля целостности. Вход в ПАК "Соболь" разрешен только администратору ПАК		
• войти в систему с использованием идентификатора администратора, вернуть исходное значение тестового ресурса или выполнить перерасчет контрольных сумм. Перезагрузить компьютер и при входе в ПАК "Соболь" предъявить идентификатор пользователя	Вход в ПАК "Соболь" выполняется успешно, отсутствуют ошибки при проверке целостности ресурсов средствами ПАК		
Проверка действия механизма замкнутой программной среды			
Если на компьютере включен в мягком режиме работы механизм замкнутой программной среды и настроен список программ и библиотек, разрешенных для запуска, — выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и запустить приложение, которое запрещено для запуска	Запуск приложения выполняется. В журнале Secret Net регистрируются события "Запрет за-		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
	пуска программы" и/или "Запрет загрузки библиотеки" (тип "Аудит отказов")		
• запустить приложение, которое разрешено для запуска	Запуск приложения выполняется. В журнале Secret Net регистрируются события "Запуск программы" и/или "Загрузка библиотеки" (тип "Аудит успехов")		
Если на компьютере включен в жестком режиме работы механизм замкнутой программной среды и настроен список программ и библиотек, разрешенных для запуска, — выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и запустить приложение, которое запрещено для запуска	Запуск приложения блокируется. В журнале Secret Net регистрируются события "Запрет запуска программы" и/или "Запрет загрузки библиотеки" (тип "Аудит отказов")		
• запустить приложение, которое разрешено для запуска	Запуск приложения выполняется. В журнале Secret Net регистрируются события "Запуск программы" и/или "Загрузка библиотеки" (тип "Аудит успехов")		
Если на компьютере включен в мягком режиме работы механизм замкнутой программной среды и настроен список исполняемых скриптов, разрешенных для запуска, — выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и запустить скрипт, которого нет в списке разрешенных для запуска	Скрипт выполняется. В журнале Secret Net регистрируется событие "Запрет исполнения неизвестного скрипта" (тип "Аудит отказов")		
• запустить скрипт, который есть в списке разрешенных для запуска	Скрипт выполняется. В журнале Secret Net регистрируется событие "Исполнение скрипта" (тип "Аудит успехов")		
Если на компьютере включен в жестком режиме работы механизм замкнутой программной среды и настроен список исполняемых скриптов, разрешенных для запуска, — выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и запустить скрипт, которого нет в списке разрешенных для запуска	Исполнение скрипта блокируется. В журнале Secret Net регистрируется событие "Запрет исполнения неизвестного скрипта" (тип "Аудит отказов")		
• запустить скрипт, который есть в списке разрешенных для запуска	Скрипт выполняется. В журнале Secret Net регистрируется событие "Исполнение скрипта" (тип "Аудит успехов")		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
Проверка действия механизма контроля подключения и изменения устройств и механизма разграничения доступа к устройствам			
В списке устройств групповой политики включить режим "Устройство не контролируется" для группы "Устройства USB". Войти в систему с учетными данными рядового пользователя и подключить новое устройство, которое не было ранее подключено к системе (например, USB-флеш-накопитель)	Устройство подключилось и работоспособно		
Подключить к компьютеру USB-устройство (например, внешний жесткий диск USB HDD). В списке устройств групповой политики включить для этого устройства режимы "Устройство постоянно подключено к компьютеру" и "Блокировать компьютер при изменении устройства". Войти в систему с учетными данными рядового пользователя и отключить устройство	Компьютер блокируется. При попытке разблокировать компьютер пользователю выдается сообщение о необходимости обратиться к администратору. Разблокировка осуществляется при вводе учетных данных администратора. В журнале Secret Net регистрируются события "Устройство удалено из системы" и "Компьютер заблокирован системой защиты" (тип "Аудит отказов"). При открытии оснастки локальной политики безопасности выводится запрос на утверждение изменений аппаратной конфигурации		
В списке устройств групповой политики включить режимы "Подключение устройства разрешено" и "Сохранять копию информации, записываемой на устройство" для класса "Устройства USB / Устройства хранения". Выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и подключить новое устройство USB-флеш-накопитель	Устройство подключилось и работоспособно. В журнале Secret Net регистрируется событие "Подключение устройства" (тип "Аудит успехов"). В оснастке локальной политики безопасности параметры для этого устройства наследуются от класса "Устройства USB / Устройства хранения"		
• войти в систему с учетными данными рядового пользователя и отключить подключенное устройство USB-флеш-накопитель	Отключение устройства не повлияло на работу системы. В журнале Secret Net регистрируется событие "Отключение устройства" (тип "Аудит успехов")		
В списке устройств групповой политики включить режим "Подключение устройства запрещено" для класса "Устройства USB / Устройства хранения". Выполнить следующие действия:			
• войти в систему с учетными данными рядового пользователя и подключить новое устройство USB-флеш-накопитель	Устройство не появилось в системе и не функционирует. В журнале Secret Net регистрируется событие "Запрет подключения устройства" (тип "Аудит отказов")		
• отключить подключенное устройство USB-флеш-накопитель	В журнале Secret Net регистрируется событие "Отключение устройства" (тип "Аудит успехов")		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
В списке устройств групповой политики включить режимы "Подключение устройства разрешено" и "Сохранять копию информации, записываемой на устройство" для устройства USB-флеш-накопитель. Вызвать диалог настройки прав доступа для устройства (с помощью кнопки "Разрешения"), добавить в список учетных записей двух пользователей, одному из которых назначить запрет записи, а другому — запрет выполнения. Выполнить следующие действия:			
• войти в систему с учетными данными пользователя, которому назначен запрет выполнения, и подключить устройство USB-флеш-накопитель. Выполнить попытки открытия файла на чтение с устройства, записи файла на устройство и запуска программы на выполнение с устройства	Устройство подключилось и работоспособно. Попытки чтения и записи файлов выполнены успешно. Запуск программы с устройства блокируется. В журнале Secret Net регистрируются события "Начата запись на сменный диск" (тип "Аудит успехов") с указанием имени файла и ссылкой на сохраненную копию и "Запрет доступа к устройству" (тип "Аудит отказов") с описанием запрошенного и разрешенного доступа		
• войти в систему с учетными данными пользователя, которому назначен запрет записи на подключенное устройство USB-флеш-накопитель. Выполнить попытки открытия файла на чтение с устройства, записи файла на устройство и запуска программы на выполнение с устройства	Попытки чтения файла и запуска программы с устройства выполнены успешно. Запись файла на устройство блокируется. В журнале Secret Net регистрируется событие "Запрет доступа к устройству" (тип "Аудит отказов") с описанием запрошенного и разрешенного доступа		
Проверка действия механизма дискреционного разграничения доступа к ресурсам файловой системы			
Если включен механизм дискреционного разграничения доступа к ресурсам файловой системы — установить для файла запреты на выполнение операций чтения, записи, выполнения и удаления одному пользователю и разрешения на те же операции другому пользователю. Выполнить следующие действия:			
• войти в систему с учетными данными пользователя, для которого установлены запреты на выполнение операций с файлом. Выполнить попытку открытия (запуска) файла	Отказ в открытии (запуске) файла с выдачей сообщения о запрете доступа. В журнале Secret Net регистрируется событие "Запрет доступа к файлу или каталогу" (тип "Аудит отказов")		
• войти в систему с учетными данными пользователя, для которого установлены разрешения на выполнение операций с файлом. Выполнить попытки открытия (запуска) файла, его изменения или удаления	Операции завершаются успешно		
Проверка действия механизма полномочного разграничения доступа			
Если включен механизм полномочного разграничения доступа и отключен режим контроля потоков — выполнить следующие действия:			
• войти в систему с учетными данными пользователя, у которого нет допуска к конфиденциальной информации. Выполнить попытку открытия документа с категорией "конфиденциально" или "строго конфиденциально"	Отказ в открытии документа с выдачей сообщения о запрете доступа. В журнале Secret Net регистрируется событие "Запрет досту-		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
	па к конфиденциальному ресурсу" (тип "Аудит отказов")		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации. Выполнить попытку открытия документа с категорией "конфиденциально"	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. В журнале Secret Net регистрируется событие "Доступ к конфиденциальному ресурсу" (тип "Аудит успехов")		
Если включен механизм полномочного разграничения доступа и включен режим контроля потоков — в списке устройств групповой политики включить режим "Устройство доступно без учета категории конфиденциальности" для устройства USB-флеш-накопитель. Выполнить следующие действия:			
• войти в систему с учетными данными пользователя, у которого нет допуска к конфиденциальной информации. Выполнить попытку открытия документа с категорией "конфиденциально" или "строго конфиденциально"	Отказ в открытии документа с выдачей сообщения о запрете доступа. В журнале Secret Net регистрируется событие "Запрет доступа к конфиденциальному ресурсу" (тип "Аудит отказов")		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации. При входе в систему выбрать уровень конфиденциальности сессии "неконфиденциально". Выполнить попытку открытия документа с категорией "конфиденциально"	Отказ в открытии документа с выдачей сообщения о запрете доступа. В журнале Secret Net регистрируется событие "Запрет доступа к конфиденциальному ресурсу" (тип "Аудит отказов") с указанием причины запрета — категория ресурса превышает уровень сессии		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Вывод конфиденциальной информации". При входе в систему выбрать уровень конфиденциальности сессии "конфиденциально". Открыть неконфиденциальный документ, изменить содержимое документа и сохранить его. Затем выполнить попытку сохранения конфиденциального документа на USB-флеш-накопитель	Документ открывается. Отказ при попытке сохранения измененного документа в каталоге без уровня конфиденциальности. Отказ при попытке сохранения конфиденциального документа на внешний носитель. В журнале Secret Net регистрируются события "Вход пользователя в систему" (тип "Аудит успехов") с указанным уровнем конфиденциальности сессии, а также "Запрет изменения параметров конфиденциальности ресурса" и "Запрет вывода конфиденциальной информации на внешний носитель" (тип "Аудит отказов")		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации и есть привилегия "Вывод конфиденциальной информации". При входе в систему выбрать уровень конфиденциальности сессии "конфиденциально". Открыть документ с категорией "конфиденциально". Изменить содержимое документа и сохранить его на USB-флеш-накопитель	Документ открывается. При сохранении документа на внешний носитель выдается предупреждение о том, что в результате выполнения данной операции будет потеряна категория конфиденциальности файла. В журнале Secret Net регистрируются события "Вход пользователя в систему" (тип "Аудит успехов") с указанным уровнем конфиденциальности сессии, а также "Доступ к конфиденциальному ресурсу" и "Вывод конфиденциальной		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
	информации на внешний носитель" (тип "Аудит успехов")		
Если включен механизм полномочного разграничения доступа и включен режим контроля потоков — в списке устройств групповой политики включить режим "Для устройства задана категория конфиденциальности" с категорией "конфиденциально" для устройства USB-флеш-накопитель. Выполнить следующие действия:			
• подключить устройство и войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Вывод конфиденциальной информации"	Вход пользователя в систему возможен только с уровнем сессии "конфиденциально" (поскольку такая категория конфиденциальности у подключенного устройства)		
• записать файл на USB-флеш-накопитель	Файл записан на USB-флеш-накопитель, и ему присвоена категория "конфиденциально". В журнале Secret Net регистрируется событие "Доступ к конфиденциальному ресурсу" (тип "Аудит успехов")		
• отключить устройство USB-флеш-накопитель и войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации. При входе в систему выбрать уровень конфиденциальности сессии "неконфиденциально". Подключить USB-флеш-накопитель	Устройство не появилось в системе и не функционирует. В журнале Secret Net регистрируется событие "Запрет подключения устройства" (тип "Аудит отказов") с указанием причины запрета — ограничение по категории конфиденциальности		
Проверка действия механизма контроля печати			
Если включен механизм полномочного разграничения доступа, отключен режим контроля потоков и отключен механизм контроля печати — выполнить следующие действия:			
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации. Открыть документ с уровнем доступа "конфиденциально". Отправить документ на печать	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. Документ печатается без маркера Secret Net. В журнале Secret Net регистрируется событие "Доступ к конфиденциальному ресурсу" (тип "Аудит успехов")		
• отправить на печать неконфиденциальный документ	Документ печатается		
Если включен механизм полномочного разграничения доступа, отключен режим контроля потоков, включен механизм контроля печати и отключен режим маркировки документов — выполнить следующие действия:			
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Печать конфиденциальных документов". Открыть документ с уровнем доступа "конфиденциально". Отправить документ на печать	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. Отказ при попытке печати документа. В журнале Secret Net регистрируются события "Доступ к конфиденциальному ресурсу" (тип "Аудит успехов") и "За-		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
	прет печати документа" (тип "Аудит отказов") с указанием причины — отсутствует привилегия		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Печать конфиденциальных документов". Открыть неконфиденциальный документ и отправить на печать	Документ печатается. В журнале Secret Net регистрируются события "Начало печати документа", "Начало печати экземпляра документа", "Успешное завершение печати экземпляра документа", "Успешное завершение печати документа" (тип "Аудит успехов")		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации и есть привилегия "Печать конфиденциальных документов". Открыть документ с уровнем доступа "конфиденциально". Отправить документ на печать	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. Документ печатается без маркера Secret Net. В журнале Secret Net регистрируются события "Доступ к конфиденциальному ресурсу", "Начало печати документа", "Начало печати экземпляра документа", "Успешное завершение печати экземпляра документа", "Успешное завершение печати документа" (тип "Аудит успехов")		
Если включен механизм полномочного разграничения доступа, отключен режим контроля потоков, включен механизм контроля печати и включен режим маркировки документов "стандартная обработка документов" или "расширенная обработка документов" — выполнить следующие действия:			
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Печать конфиденциальных документов". Открыть документ с уровнем доступа "конфиденциально". Отправить документ на печать	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. Отказ при попытке печати документа. В журнале Secret Net регистрируются события "Доступ к конфиденциальному ресурсу" (тип "Аудит успехов") и "Запрет печати документа" (тип "Аудит отказов") с указанием причины — отсутствует привилегия		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации, но нет привилегии "Печать конфиденциальных документов". Открыть неконфиденциальный документ и отправить на печать	Документ печатается. В журнале Secret Net регистрируются события "Начало печати документа", "Начало печати экземпляра документа", "Успешное завершение печати экземпляра документа", "Успешное завершение печати документа" (тип "Аудит успехов")		
• войти в систему с учетными данными пользователя, у которого есть допуск к конфиденциальной информации и есть привилегия "Печать конфиденциальных документов". Открыть документ с уровнем доступа "конфиденциально". Отправить документ на печать	Документ открывается. При открытии документа выдается сообщение о повышении уровня конфиденциальности приложения. Документ печатается с маркером Secret Net (с предварительным запросом значений для настраиваемых полей маркера). В журнале Secret Net регистрируются события "Доступ к конфиденциальному ресурсу", "Начало печати документа",		

Действие	Ожидаемый результат	Подлежит выполнению	Отметка о выполнении
	"Начало печати экземпляра документа", "Успешное завершение печати экземпляра документа", "Успешное завершение печати документа" (тип "Аудит успехов")		
Проверка централизованного сбора локальных журналов Secret Net (для сетевого варианта СЗИ)			
На рабочем месте администратора запустить программу оперативного управления в режиме мониторинга и централизованного аудита и выполнить следующие действия:			
• выбрать в списке включенную рабочую станцию, вызвать контекстное меню и выбрать команду "Запросы / Журналы станций / Secret Net"	Журнал Secret Net для рабочей станции загружается из базы данных		
• выбрать в списке включенную рабочую станцию, вызвать контекстное меню и выбрать команду "Команды / Оперативные команды / Собрать журналы / Secret Net". После окончания процесса сбора локального журнала вызвать контекстное меню рабочей станции и выбрать команду "Запросы / Журналы станций / Secret Net"	В программу загружается обновленный журнал с новыми записями, поступившими из локального журнала рабочей станции		
Проверка мониторинга компьютеров (для сетевого варианта СЗИ)			
На рабочем месте администратора оперативного управления запустить программу оперативного управления в режиме мониторинга и централизованного аудита. Проверить отображение активного состояния для включенной рабочей станции. На самой рабочей станции выполнить попытку входа пользователя с указанием неправильного пароля (при этом в ОС Windows должна быть включена регистрация событий входа/выхода, имеющих тип "Аудит отказов") или с предъявлением неправильного идентификатора	При запуске программы оперативного управления осуществляется соединение с сервером безопасности и загружается структура оперативного управления. Отображение состояния рабочих станций соответствует действительности. Запись о зарегистрированном событии НСД на рабочей станции отображается в списке событий панели "События системы"		
Проверка оперативного управления компьютерами (для сетевого варианта СЗИ)			
На рабочем месте администратора оперативного управления запустить программу оперативного управления в режиме мониторинга и централизованного аудита и выполнить следующие действия:			
• выбрать в списке включенную рабочую станцию, вызвать контекстное меню и выбрать команду "Команды / Оперативные команды / Заблокировать"	Включенная рабочая станция блокируется. Разблокировка рабочей станции может быть выполнена только по команде из программы оперативного управления или локально при вводе учетных данных администратора		
• выбрать в списке включенную рабочую станцию и в панели свойств объектов перейти на вкладку "Локальные политики". В списке параметров политик отредактировать одно или несколько значений	В программу загружается список параметров локальной политики безопасности. Сделанные изменения сохранены в программе оперативного управления и применены на рабочей станции (отображаются в оснастке локальной политики безопасности)		