ГАЗИНФОРМ СЕРВИС

Программный комплекс управления конфигурациями и анализа защищенности «Efros Config Inspector» v.3

Руководство администратора. Приложение 1

Санкт-Петербург, 202

Содержание

1 Регламентное тестирование ПК «Efros Config Inspector» v.3.1

Программа проведения регламентного тестирования приведена в таблице 1.

Таблица 1 – Программа проведения регламентного тестирования ПК ««Efros Config Inspector» v.3.1»

№ п/п	Наименование испытаний (проверок)	Пункт методики
1	Проверка механизма идентификации и аутентификации субъектов доступа	1.1
	Проверка требования от пользователей идентифицировать себя при доступе к серверу ПК и проверка подлинности идентификатора субъекта (аутентификации)	1.1.1
	Проверка требования от пользователей идентифицировать себя при доступе к контролируемому на сервере ПК оборудованию	1.1.2
	Проверка механизма управления идентификаторами пользователей на сервере ПК	1.1.3
	Проверка механизма управления средствами аутентификации пользователей на сервере ПК	1.1.4
	Проверка защиты обратной связи механизма аутентификации ПК	1.1.5
2	Проверка механизма управления доступом субъектов доступа к объектам доступа	1.2
	Проверка реализации механизма управления учетными записями пользователей комплекса	1.2.1
	Проверка реализации ролевого метода управления доступом и типов (чтение, запись, выполнение) разграничения доступа	1.2.2
	Проверка реализации механизма разделения полномочий пользователей и администраторов ПК	1.2.3
	Проверка реализации требования по назначению минимально необходимых прав и привилегий пользователям и администраторам ПК	1.2.4
	Проверка ограничения неуспешных попыток входа пользователя на сервер ПК	1.2.5
	Проверка ограничения количества параллельных сеансов доступа для учетной записи пользователя ПК	1.2.6
3	Проверка анализа защищенности информации	1.3
	Проверка выявления, анализа и устранения уязвимостей контролируемого оборудования	1.3.1
	Проверка контроля установки обновлений программного обеспечения на контролируемом на сервере ПК оборудовании.	1.3.2
	Проверка контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения контролируемого оборудования.	1.3.3
	Проверка выполнения контроля состава технических средств и программного обеспечения контролируемого оборудования.	1.3.4
	Проверка выполнения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей программного комплекса.	1.3.5
4	Проверка выполнения контроля целостности программного обеспечения контролируемого на сервере ПК оборудования	1.4
5	Проверка выполнения контроля целостности виртуальной инфраструктуры и ее конфигураций	1.5
6	Проверка регистрации событий безопасности	1.6
7	Проверка управления конфигурациями контролируемого оборудования с сервера ПК	1.7
	Проверка управления изменениями конфигурации сетевого оборудования	1.7.1

№ п/п	Наименование испытаний (проверок)	Пункт методики
	Проверка регистрации данных об изменениях в конфигурации сетевого оборудования	1.7.2

1.1 Проверка механизма идентификации и аутентификации субъектов доступа

1.1.1 Проверка требования от пользователей идентифицировать себя при доступе к серверу ПК и проверка подлинности идентификатора субъекта (аутентификации)

Описание функции:

Идентификация и аутентификация пользователя при его доступе к серверу ПК предназначена для защиты сервера ПК от изменения параметров сервера ПК незарегистрированным пользователем. Данный механизм предполагает наличие у пользователя уникального регистрационного имени и пароля.

На сервере ПК ведется список пользователей, которым разрешен доступ к серверу ПК, который может быть изменен администратором безопасности. Идентификация и аутентификация пользователей осуществляются в момент доступа пользователя к серверу ПК из клиентской консоли.

Действия:

С помощью клиентской консоли осуществляется авторизация пользователя на сервере ПК. Последовательность действий для проверки приведена в таблице 2.

Таблица 2 – Проверка корректности идентификации и аутентификации пользователя при подключении к серверу ПК

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ CONSOL	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user2** и нажать кнопку ***Подключиться***	Ошибка подключения к серверу ПК
3	В окне подключения консоли к серверу ПК ввести логин учетной записи администратора комплекса root, поле ***Пароль*** оставить пустым и нажать кнопку ***Подключиться***	Ошибка подключения к серверу ПК
4	В окне подключения консоли к серверу ПК отметить параметр ***Вход под текущим пользователем*** и нажать кнопку ***Подключиться***	Ошибка подключения к серверу ПК

№ п/п	Действия	Ожидаемый результат
5	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса root и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
6	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих попытки авторизации пользователей на сервере ПК.

Критерии оценки:

Результаты проверки считаются положительным, если:

– при вводе имени зарегистрированного на сервере ПК пользователя и верного пароля осуществляется подключение к серверу ПК;

– при вводе незарегистрированного на сервере ПК имени пользователя или вводе неверного пароля появляется сообщение об ошибке данных аутентификации;

– сервер ПК обеспечивает надежную регистрацию всех событий, связанных с попытками идентификации и аутентификации.

1.1.2 Проверка требования от пользователей идентифицировать себя при доступе к контролируемому на сервере ПК оборудованию

Описание функции:

Идентификация и аутентификация пользователя при его доступе к контролируемому на сервере ПК оборудованию предназначена для защиты доступа к конфигурации оборудования незарегистрированного пользователя. Данный механизм предполагает наличие у пользователя уникального регистрационного имени и пароля.

Действия:

С помощью клиентской консоли на сервер ПК добавляется оборудование для контроля и выполняется последовательность действий для проверки авторизации пользователей на нем (таблица 3).

Таблица 3 – Проверка корректности идентификации и аутентификации пользователя при подключении к контролируемому на сервере ПК оборудованию

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ **CONSOL**	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса root и нажать кнопку **Подключиться**	Открытие клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
4	В форме управления внешними модулями комплекса нажать на переключатель ***Подключить*** для модуля ***Поддержка сетевых устройств Cisco***	Открытие окна ***«Поддержка сетевых устройств Cisco»***
5	В окне ***«Поддержка сетевых устройств Cisco»*** отметить параметр ***Разрешить сохранение логов*** и нажать кнопку ***Сохранить***	Возврат в форму управления внешними модулями комплекса. Модуль ***Поддержка сетевых устройств Cisco подключен***
6	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна ***«Новое устройство»***
7	В окне ***«Новое устройство»*** заполнить все поля, определяющие добавляемое на сервер ПК устройство, в поле Пользователь ввести имя (логин) незарегистрированного на устройстве пользователя и нажать кнопку ***Проверить подключение***	Ошибка выполнения операции ***Проверка соединения***
8	В поле Пользователь окна «Новое устройство» ввести имя пользователя, зарегистрированного на устройстве, в поле Пароль ввести неверный пароль указанного пользователя и нажать кнопку ***Проверить*** подключение	Ошибка выполнения операции Проверка соединения
9	В поля ***Пользователь*** и ***Пароль*** окна ***«Новое устройство»*** ввести имя и верный пароль пользователя, зарегистрированного на устройстве, и нажать кнопку ***Проверить подключение***	Успешное выполнения операции ***Проверка соединения***
10	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих попытки авторизации пользователя на контролируемом на сервере ПК устройстве.

Критерии оценки:

Результаты проверки считаются положительным, если:

– при вводе имени, зарегистрированного на контролируемом на сервере ПК устройстве пользователя и верного пароля, осуществляется подключение сервера ПК к устройству;

– при вводе незарегистрированного на контролируемом на сервере ПК устройстве имени пользователя или вводе неверного пароля этого пользователя соединение сервера ПК с устройством не происходит;

– ПК обеспечивает надежную регистрацию всех событий, связанных с попытками идентификации и аутентификации пользователей на контролируемом на сервере ПК оборудовании.

1.1.3 Проверка механизма управления идентификаторами пользователей на сервере ПК

Описание функции:

Механизм управления идентификаторами пользователей в ПК «Efros Config Inspector» v.3.1 предназначен для однозначной идентификации пользователя при его авторизации на сервере ПК.

Действия:

С помощью клиентской консоли на сервере ПК регистрируется группа пользователей с указанными ниже параметрами учетных записей и выполняется последовательность действий для проверки (таблица 4).

Таблица 4 – Управление учетными записями пользователей в клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
1	Проверка возможности добавления учетных записей пользователей	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса root и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области Администрирование нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
1.5	В форме управления пользователями системы и их правами нажать кнопку ***Добавить***	Открытие окна ***«Добавление нового пользователя»***
1.6	В окне ***«Добавление нового пользователя»***: - в поле ***Логин*** ввести **user1**; - в поля ***Пароль*** и ***Повторите пароль*** ввести пароль учетной записи **user1**; - отметить параметры ***Администратор, Чтение, Запись, Выполнение;*** - нажать кнопку ***Сохранить***.	Отображение в списке пользователей формы управления пользователями системы и их правами добавленной учетной записи user1
1.7	Повторить действия п. 1.5 и 1.6 для учетных записей user2 (роль: ***Опытный пользователь***, права: ***Чтение, Запись, Выполнение***) и **user3** (роль: ***Пользователь, права: Чтение, Выполнение***)	Отображение в списке пользователей формы управления пользователями системы и их правами добавленных учетных записей **user2** и **user3**
2	Проверка возможности изменения имени учетной записи пользователя ПК	
2.1	В форме управления пользователями системы и их правами нажать ссылку ***Изменить*** для учетной записи **user3**	Появление окна ***«Изменение пользователя»***

№ п/п	Действия	Ожидаемый результат
2.2	В окне ***«Изменение пользователя»*** изменить имя пользователя **user3** на **user2** и нажать кнопку ***Сохранить***	Ошибка внесения изменений в параметры учетной записи ***user3*** на сервере ПК – имя пользователя не изменяется
2.3	Изменить имя пользователя **user3** на **user4**	Успешное изменение имени пользователя.
2.5	В форме управления пользователями системы и их правами нажать ссылку ***Заблокировать*** для учетной записи **user4**	Успешная блокировка пользователя **user4**, ссылка изменилась на Разблокировать
2.6	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих изменение настроек на сервере ПК.
3	Проверка идентификации и аутентификации пользователей на сервере ПК	
3.1	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user2** и нажать кнопку ***Подключиться***	Ошибка подключения к серверу ПК
3.2	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user4.** Указать неверный пароль.	Ошибка подключения к серверу ПК
3.3	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user4**. Указать верный пароль.	Ошибка подключения к серверу ПК
3.4	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user1.** Указать верный пароль.	Открытие окна изменения пароля пользователем «Требуется изменить временный пароль»
3.5	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, состоящий из восьми символов и отличающийся от пароля, назначенного пользователю администратором комплекса и нажать кнопку **Сохранить**	Открытие клиентской консоли ПК
4	Просмотр списка событий в локальной консоли программного комплекса	
4.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих попытки подключения пользователей к серверу ПК.

Критерии оценки:

Результаты проверки считаются положительным, если:

– при попытке подключения пользователя к серверу ПК осуществляется его однозначная идентификация;

– при вводе имени незарегистрированного или заблокированного на сервере ПК пользователя, при вводе неверного пароля пользователя появляется сообщение об ошибке данных аутентификации;

– ПК обеспечивает надежную регистрацию всех событий, связанных с попытками идентификации и аутентификации пользователей на сервере ПК.

1.1.4 Проверка механизма управления средствами аутентификации пользователей на сервере ПК

Описание функции:

Механизм управления средствами аутентификации пользователей в ПК «Efros Config Inspector» v.3.1 определяет следующие требования к характеристикам паролей пользователей ПК:

а) минимальная сложность пароля с установленными требованиями к количеству символов, сочетанию букв верхнего и нижнего регистра, цифр и специальных символов;
б) задание минимального количества измененных символов при создании новых паролей;
в) задание максимального времени действия пароля;
г) задание минимального времени действия пароля;
д) запрет на использование пользователями ПК любого из ранее использованных паролей при создании новых паролей;

Также на сервере ПК осуществляется блокировка на 15 минут программно-технического средства, с которого осуществляется доступ на сервер ПК, в случае четырехкратного ввода неверной идентификационной информации пользователя ПК.

Действия:

Последовательность действий по проверке механизма управления средствами аутентификации пользователей на сервере ПК приведена в таблице 5.

Таблица 5 – Управление средствами аутентификации пользователей в ПК «Efros Config Inspector» v.3.1

№ п/п	Действия	Ожидаемый результат
1	Проверка сложности паролей пользователей ПК	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области *Администрирование* нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.

№ п/п	Действия	Ожидаемый результат
1.5	В форме управления пользователями системы и их правами нажать ссылку ***Разблокировать*** для учетной записи **user4**	Успешная разблокировка пользователя **user4**, ссылка изменилась на Заблокировать
1.6	Выйти из клиентской консоли. В заголовке клиентской консоли нажать на имя работающего с консолью пользователя **root** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
1.7	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user4**. Указать верный пароль.	Открытие окна изменения пароля пользователем «***Требуется изменить временный пароль***»
1.8	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, состоящий из семи символов	Кнопка ***Сохранить*** неактивна. Сообщение об ошибке: ***Длина пароля менее 8 символов***.
1.9	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, состоящий из восьми цифр	Кнопка ***Сохранить*** неактивна. Сообщение об ошибке: ***Алфавит пароля менее 60 символов***.
1.10	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, начинающийся на **user4**	Кнопка ***Сохранить*** неактивна. Сообщение об ошибке: ***Пароль начинается с имени пользователя***.
1.11	В поля ввода окна «Требуется изменить временный пароль» ввести пароль, который назначил пользователю администратор комплекса	Кнопка ***Сохранить*** неактивна. Сообщение об ошибке: ***Отличие от предыдущего пароля менее 3 символов***.
1.12	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, состоящий из восьми символов и отличающийся от пароля, назначенного пользователю администратором комплекса и нажать кнопку ***Сохранить***	Открытие клиентской консоли ПК
1.13	Выйти из клиентской консоли. В заголовке клиентской консоли нажать на имя работающего с консолью пользователя **user4** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
2	Проверка автоматической блокировки устройства, с которого осуществляется подключение к серверу ПК	
2.1	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя ***user2*** и нажать кнопку Подключиться	Ошибка подключения к серверу ПК

№ п/п	Действия	Ожидаемый результат
2.2	Повторить попытки подключения к серверу ПК еще три раза	Ошибка подключения к серверу ПК
2.3	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя ***user1***. Указать верный пароль	Блокировка возможности подключения к серверу ПК с текущего IP-адреса
2.4	Через 15 минут выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя ***user1***. Указать верный пароль	Открытие клиентской консоли ПК
3	Проверка возможности изменения пароля пользователями без привлечения администратора комплекса	
3.1	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***user1*** и в открывшемся контекстном меню выбрать пункт ***Сменить пароль***	Открытие окна **«Сменить пароль текущего пользователя»**
3.2	Заполнить поля окна **«Сменить пароль текущего пользователя»**: - в поле ввода ***Текущий пароль*** ввести текущий пароль; - в поле ввода ***Новый пароль*** ввести новый пароль (длиной 7 символов); - повторить ввод нового пароля в поле ввода ***Повторите пароль***.	Кнопка ***Сохранить*** неактивна. Сообщение об ошибке: ***Длина пароля менее 8 символов***
3.3	В окне **«Сменить пароль текущего пользователя»**: - в поле ввода ***Новый пароль*** ввести новый пароль (длиной 8 символов); - повторить ввод нового пароля в поле ввода ***Повторите пароль***. Нажать кнопку ***Сохранить***	Ошибка смены пароля
3.4	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
3.5	В области ***Администрирование*** нажать ссылку ***Настройки,*** расположенную под кнопкой ***Пользователи***	Открытие окна ***«Настройки пользователей»***
3.6	В окне ***«Настройки пользователей»*** снять отметку с параметра ***Ограничение времени действия паролей*** и нажать кнопку ***Сохранить***	Возврат в раздел Настройки клиентской консоли ПК
3.7	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***user1*** и в открывшемся контекстном меню выбрать пункт ***Сменить пароль***	Открытие окна **«Сменить пароль текущего пользователя»**

№ п/п	Действия	Ожидаемый результат
3.8	В окне **«Сменить пароль текущего пользователя»**: - в поле ввода Новый пароль ввести новый пароль (длиной 8 символов); - повторить ввод нового пароля в поле ввода ***Повторите пароль***. Нажать кнопку ***Сохранить***	Пароль изменен
3.9	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***user1*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
3.10	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя ***user1***. Указать пароль, состоящий из 7 символов	Ошибка подключения к серверу ПК
3.11	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя ***user1***. Указать верный пароль	Открытие клиентской консоли ПК
4	Проверка возможности изменения пароля пользователя ПК администратором комплекса	
4.1	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
4.2	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
4.3	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
4.4	В форме управления пользователями системы и их правами нажать ссылку ***Сменить пароль*** для учетной записи ***user1***	Открытие окна «**Сменить пароль пользователя user1**»
4.5	В поля ввода окна «**Сменить пароль пользователя user1**» ввести новый пароль и нажать кнопку ***Сохранить***	Пароль пользователя ***user1*** изменен
4.6	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
4.7	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами	Ошибка подключения к серверу ПК

№ п/п	Действия	Ожидаемый результат
	пользователя ***user1*** с указанием старого пароля	
4.8	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами пользователя ***user1*** с указанием старого пароля	Открытие окна изменения пароля пользователем «**Требуется изменить временный пароль**»
4.9	В поля ввода окна «**Требуется изменить временный пароль**» ввести пароль, состоящий из восьми символов и отличающийся от пароля, назначенного пользователю администратором комплекса и нажать кнопку ***Сохранить***	Открытие клиентской консоли ПК
4.10	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***user1*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
5	Проверка возможности блокировки пользователей на сервере ПК	
5.1	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
5.2	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
5.3	В области Администрирование нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
5.4	В форме управления пользователями системы и их правами нажать ссылку ***Заблокировать*** для учетной записи ***user1***	Ссылка изменила свое значение на ***Разблокировать***
5.5	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
5.6	Попытаться подключиться к серверу ПК от имени и с правами пользователя ***user1***	Ошибка подключения к серверу ПК
5.7	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
5.8	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
5.9	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.

№ п/п	Действия	Ожидаемый результат
5.10	В форме управления пользователями системы и их правами нажать ссылку ***Разблокировать*** для учетной записи ***user1***	Ссылка изменила свое значение на Заблокировать
5.11	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
5.12	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***user1*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
6	Просмотр списка событий в локальной консоли программного комплекса	
6.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих операции блокировки (разблокировки) пользователя и попытки подключения пользователей к серверу ПК.

Критерии оценки:

Результаты проверки считаются положительным, если:

– на сервере ПК блокируется возможность задания пароля пользователя, не удовлетворяющего установленным требованиям к его сложности;

– при четырехкратном вводе неверной идентификационной информации в процессе авторизации пользователя на сервере ПК возможность подключения к серверу ПК для используемой ПЭВМ блокируется на 15 минут;

– сервер ПК обеспечивает надежную регистрацию всех событий, связанных с работой механизма управления средствами аутентификации.

1.1.5 Проверка защиты обратной связи механизма аутентификации ПК

Описание функции:

В ПК «Efros Config Inspector» v.3.1 в процессе аутентификации пользователя на сервере ПК обеспечивается защита обратной связи «сервер ПК – пользователь», заключающаяся в исключении отображения для пользователя действительного значения идентификационной информации.

Действия:

Последовательность действий по проверке защиты обратной связи механизма аутентификации ПК приведена в пунктах 1.1.1 и 1.1.2. Символы пароля, вводимые в окне подключения к консоли и в окне добавления устройства, отображаются условными знаками «·».

Критерии оценки:

Результаты проверки считаются положительным, если при вводе пароля его значение скрыто от пользователя.

1.2 Проверка механизма управления доступом субъектов доступа к объектам доступа

1.2.1 Проверка реализации механизма управления учетными записями пользователей комплекса

Описание функции:

На сервере ПК «Efros Config Inspector» v.3.1 осуществляется заведение, активация, блокирование и уничтожение учетных записей пользователей программного комплекса. Предоставление пользователям комплекса прав доступа к контролируемым устройствам осуществляется, основываясь на задачах, решаемых пользователями ПК. На сервере ПК осуществляется автоматическое блокирование неактивных (неиспользуемых) учетных записей пользователей комплекса после 45 дней неиспользования.

Действия:

Последовательность действий по проверке механизма управления учетными записями пользователей на сервере ПК приведена в таблице 6.

Таблица 6 – Управление учетными записями пользователей на сервере ПК «Efros Config Inspector» v.3.1

№ п/п	Действия	Ожидаемый результат
1	Проверка операции добавления пользователей на сервер ПК	
1.1	Запустить клиентскую консоль ПК на ЭВМ CONSOL	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root и*** нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
1.5	В форме управления пользователями системы и их правами нажать кнопку ***Добавить***	Открытие окна «***Добавление нового пользователя***»

№ п/п	Действия	Ожидаемый результат
1.6	В окне «**Добавление нового пользователя**»: - в поле ***Логин*** ввести ***user5***; - в поля ***Пароль*** и ***Повторите пароль*** ввести пароль учетной записи ***user5***; - отметить параметры ***Пользователь, Чтение;*** - нажать кнопку ***Сохранить***.	Отображение в списке пользователей формы управления пользователями системы и их правами добавленной учетной записи ***user5***
1.7	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
1.8	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя ***user5.*** Указать верный пароль.	Открытие окна изменения пароля пользователем «***Требуется изменить временный пароль***»
1.9	В поля ввода окна «***Требуется изменить временный пароль***» ввести пароль, состоящий из восьми символов и отличающийся от пароля, назначенного пользователю администратором комплекса и нажать кнопку ***Сохранить***	Открытие клиентской консоли ПК
1.10	В панели выбора раздела клиентской консоли ПК нажать кнопку ***События***	Отображение сообщений аудита, фиксирующих операции добавления пользователя на сервер ПК, попытки подключения пользователя к серверу ПК и смены пароля пользователя.
1.11	Выйти из клиентской консоли. В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
2	Проверка возможности блокировки пользователей на сервере ПК	
2.1	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
2.2	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
2.3	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
2.4	В форме управления пользователями системы и их правами в контекстном меню пользователя выбрать пункт	Пункт контекстного меню измениться на ***Разблокировать***

№ п/п	Действия	Ожидаемый результат
	Заблокировать для учетной записи ***user5***	
2.5	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
2.6	Попытаться подключиться к серверу ПК от имени и с правами пользователя ***user5***	Ошибка подключения к серверу ПК
2.7	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
2.8	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
2.9	В области Администрирование нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
2.10	В форме управления пользователями системы и их правами в контекстном меню пользователя выбрать пункт ***Разблокировать*** для учетной записи ***user5***	Пункт контекстного меню измениться на ***Заблокировать***
2.11	В заголовке клиентской консоли нажать на имя работающего с консолью пользователя ***root*** и в открывшемся контекстном меню выбрать пункт ***Выход***	Открытие окна подключения консоли к серверу ПК
2.12	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи ***user5*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
3	Проверка возможности удаления пользователей с сервера ПК	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
3.2	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
3.2	В форме управления пользователями системы и их правами нажать ссылку ***Удалить*** для учетной записи ***user5***	Открытие окна «**Удалить пользователя**»
3.4	В окне «***Удалить пользователя***» нажать кнопку **Удалить**	Ошибка выполнения операции удаления пользователя с сервера ПК
3.5	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК

№ п/п	Действия	Ожидаемый результат
3.6	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
3.7	В области ***Администрирование*** нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
3.8	В форме управления пользователями системы и их правами нажать ссылку ***Удалить*** для учетной записи ***user5***	Открытие окна «Удалить пользователя»
3.9	В окне «Удалить пользователя» нажать кнопку Удалить	Успешное удаление пользователя с сервера ПК
3.10	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
3.11	Попытаться подключиться к серверу ПК от имени и с правами удаленного пользователя ***user5***	Ошибка подключения к серверу ПК
4	Проверка автоматической блокировки пользователей на сервере ПК	
4.1	На сервере ПК (ЭВМ SERVER) изменить системную дату, увеличив ее на 46 дней от текущей даты	Системная дата успешно изменена
4.2	Запустить серверную консоль и в области ***Служба сервера*** нажать кнопку ***Стоп***	Служба сервера ПК остановлена
4.3	В окне серверной консоли в области ***Служба сервера*** нажать кнопку ***Старт***	Служба сервера ПК запущена
4.4	На ЭВМ CONSOLE запустить клиентскую консоль и осуществить попытку подключения к серверу ПК от имени учетной записи ***user1***	Ошибка подключения к серверу ПК
4.5	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса ***root*** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
4.6	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройки***	В рабочей области консоли отобразился список параметров сервера ПК
4.7	В области Администрирование нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
4.8	В форме управления пользователями системы и их правами навести указатель мыши на иконку учётной записи пользователя ***user1***	Появление всплывающего сообщения Пользователь заблокирован
4.9	В форме управления пользователями системы и их правами нажать ссылку ***Разблокировать*** для учетной записи ***user1***	Ссылка изменила свое значение на ***Заблокировать***

№ п/п	Действия	Ожидаемый результат
4.10	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
4.11	Попытаться подключиться к серверу ПК от имени и с правами пользователя ***user1***	Открытие клиентской консоли ПК
4.12	В панели выбора раздела клиентской консоли ПК нажать кнопку События	Отображение сообщений аудита, фиксирующих операции удаления, автоматической блокировки пользователей, попытки подключения пользователей к серверу ПК.

Критерии оценки:

Результаты проверки считаются положительным, если:

– на сервере ПК осуществляется возможность добавления пользователей, их блокировки, активации и удаления;
– на сервере ПК осуществляется автоматическая блокировка учетной записи пользователя в случае ее длительного неиспользования.

1.2.2 Проверка реализации ролевого метода управления доступом и типов (чтение, запись, выполнение) разграничения доступа

Описание функции:

На сервере ПК реализован ролевой метод управления доступом, предусматривающий доступ пользователей комплекса к администрированию параметров сервера ПК, параметров контроля устройств на основе ролей пользователей ПК. На сервере ПК реализованы типы доступа, включающие операции по чтению, записи (удалению), выполнению, разрешенные к выполнению пользователям ПК при доступе к контролируемым устройствам.

Действия:

Последовательность действий по проверке ролевого метода управления доступом и типов разграничения доступа пользователей на сервере ПК приведена в таблице 7.

Таблица 7 – Ролевой метод и типы разграничения доступа пользователей к контролируемым на сервере ПК устройствам

№ п/п	Действия	Ожидаемый результат
1	Проверка возможности администрирования параметров сервера ПК	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль	Открытие клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
	учетной записи администратора комплекса **user1** (роль **Администратор**) и нажать кнопку ***Подключиться***	
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области *Администрирование* нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
1.5	В форме управления пользователями системы и их правами нажать кнопку ***Добавить***	Открытие окна **«Добавление нового пользователя»**
1.6	В окне **«Добавление нового пользователя»**: - в поле ***Логин*** ввести **user5**; в поля ***Пароль*** и ***Повторите пароль*** ввести пароль учетной записи **user5**; отметить параметры ***Пользователь***, ***Чтение***; - нажать кнопку ***Сохранить***.	Отображение в списке пользователей формы управления пользователями системы и их правами добавленной учетной записи **user5**
1.7	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
1.8	В области *Администрирование* нажать кнопку ***База данных***	Открытие окна **«База данных»**.
1.9	В открывшемся окне изменить срок хранения отчетов в архиве и нажать кнопку ***Сохранить***	Успешное изменение срока хранения отчетов в архиве, возврат во вкладку **Настройки**
1.10	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
1.11	Выполнить подключение к серверу ПК от имени и с правами пользователя **user2** (роль **Опытный пользователь**)	Открытие клиентской консоли ПК
1.12	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК.
1.13	В области *Администрирование* нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами невозможно. Кнопка выбора настроек заблокированы. Изменить настройки невозможно.
1.14	В области *Администрирование* нажать кнопку ***База данных***	Кнопка выбора настроек заблокированы. Изменить настройки невозможно.
1.15	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
1.16	Выполнить подключение к серверу ПК от имени и с правами пользователя **user4** (роль **Пользователь**)	Открытие клиентской консоли ПК
1.17	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК

№ п/п	Действия	Ожидаемый результат
1.18	В области *Администрирование* нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами. Кнопка выбора настроек заблокированы. Изменить настройки невозможно.
1.19	В области *Администрирование* нажать кнопку ***База данных***	Кнопка выбора настроек заблокированы. Изменить настройки невозможно.
2	Проверка возможности изменения параметров контроля устройств	
2.1	Выполнить подключение к серверу ПК от имени и с правами пользователя **user1** (роль **Администратор**)	Открытие клиентской консоли ПК
2.2	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
2.3	В окне **«Новое устройство»** заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства в список контролируемых на сервере ПК
2.4	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК
2.5	В области *Настройки контроля* нажать кнопку ***Отчеты***	Открытие формы создания и настройки использования отчетов, предназначенных для загрузки с контролируемых устройств
2.6	В форме настройки отчетов нажать кнопку ***Добавить***	Открытие окна **«Новый отчет»**
2.7	В окне **«Новый отчет»** ввести контролируемые параметры устройства, ввести команду ***show version***, отметить параметры ***Разрешить использование*** и ***Включить контроль целостности*** и кнопку нажать ***Сохранить***	Закрытие окна **«Новый отчет».** Успешное добавление нового отчета, возврат в форму создания и настройки использования отчетов
2.8	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
2.9	Выполнить подключение к серверу ПК от имени и с правами пользователя **user2** (роль **Опытный пользователь**)	Открытие клиентской консоли ПК
2.10	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
2.12	В окне **«Новое устройство»** заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства, ввести идентификационные данные учетной записи пользователя для	Успешное добавление устройства в список контролируемых на сервере ПК

№ п/п	Действия	Ожидаемый результат
	авторизации на устройстве и нажать кнопку ***Добавить***	
2.13	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК
2.14	В области *Настройки контроля* нажать кнопку ***Отчеты***	Открытие формы создания и настройки использования отчетов, предназначенных для загрузки с контролируемых устройств
2.15	В форме настройки отчетов нажать кнопку ***Добавить***	Открытие окна **«Новый отчет»**
2.16	В окне **«Новый отчет»** выделить тип добавляемого отчета, ввести контролируемые параметры устройства, необходимые параметры использования отчета и нажать кнопку ***Сохранить***	Успешное добавление нового отчета, возврат в форму создания и настройки использования отчетов
2.17	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
2.18	Выполнить подключение к серверу ПК от имени и с правами пользователя **user4** (роль **Пользователь**, права ***Чтение*** и ***Выполнение***)	Открытие клиентской консоли ПК
2.19	В локальной консоли перейти на вкладку **Устройства** и нажать кнопку ***Добавить устройство***	Кнопка ***Добавить устройство*** заблокирована. Добавить устройство невозможно.
2.20	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК
2.21	В области **Настройки** сервера нажать кнопку ***Отчеты***	Ошибка открытия вкладки отчеты. Кнопка ***Отчеты*** неактивна.
2.22	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
3	Просмотр сообщений аудита	
3.1	Выполнить подключение к серверу ПК от имени и с правами пользователя **user1** (роль **Администратор**)	Открытие клиентской консоли ПК
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих операции изменения параметров сервера ПК и параметров контроля устройств на сервере ПК

Критерии оценки:

Результаты проверки считаются положительным, если:

– на сервере ПК осуществляется управление доступом пользователей к администрированию сервера ПК на основе присвоенных им ролей;
– доступ пользователей к контролируемым на сервере ПК устройствам осуществляется на основании назначенных пользователю прав.

1.2.3 Проверка реализации механизма разделения полномочий пользователей и администраторов ПК

Описание функции:

На сервере ПК реализован механизм разделения полномочий пользователей ПК по осуществлению администрирования параметров сервера ПК и контроля устройств в соответствии с должностными обязанностями (функциями) пользователей ПК.

Действия:

Последовательность действий по проверке реализации на сервере ПК механизма разделения полномочий пользователей ПК приведена в таблице 8.

Таблица 8 – Разделение полномочий пользователей и администраторов ПК

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи администратора комплекса **user1** (роль **Администратор**) и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
4	В области *Администрирование* нажать кнопку ***Пользователи***	Открытие формы управления пользователями системы и их правами.
5	В форме управления пользователями системы и их правами нажать кнопку ***Добавить***	Открытие окна **«Добавление нового пользователя»**
6	В окне **«Добавление нового пользователя»**: - в поле ***Логин*** ввести **user6**; - в поля ***Пароль*** и ***Повторите пароль*** ввести пароль учетной записи **user6**; - отметить параметр ***Администратор***; - остальные параметры оставить неотмеченными - нажать кнопку ***Сохранить***.	Отображение в списке пользователей формы управления пользователями системы и их правами добавленной учетной записи **user6**
7	Выйти из клиентской консоли	Открытие окна подключения консоли к серверу ПК
8	Выполнить подключение к серверу ПК от имени и с правами пользователя **user6** (роль **Администратор**)	Открытие окна изменения пароля пользователем **«Требуется изменить временный пароль»**
9	В поля ввода окна **«Требуется изменить временный пароль»** ввести пароль, состоящий из восьми	Открытие клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
	символов и отличающийся от пароля, назначенного пользователю администратором комплекса и нажать кнопку ***Сохранить***	
10	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается пустая рабочая область: в списке отсутствуют контролируемые устройства (группы)
11	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
12	В области *Администрирование* нажать ссылку ***Настройки***, расположенную под кнопкой ***Пользователи***	Открытие окна **«Настройки пользователей»**.
13	В окне **«Настройки пользователей»** изменить параметры безопасности учетных записей пользователей на сервере ПК и нажать кнопку ***Сохранить***	Успешное изменение параметров безопасности учетных записей пользователей на сервере ПК, возврат во вкладку **Настройки**
14	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих операции изменения параметров сервера ПК

Критерии оценки:

Результаты проверки считаются положительным, если на сервере ПК осуществляется разделение полномочий пользователей ПК по осуществлению администрирования параметров сервера ПК и контроля устройств.

1.2.4 Проверка реализации требования по назначению минимально необходимых прав и привилегий пользователям и администраторам ПК

Описание функции:

На сервере ПК реализовано требование по предоставлению прав и привилегий по доступу к параметрам настройки программного комплекса исключительно администратору, наделенному соответствующими полномочиями.

Действия:

Последовательность действий по проверке реализации на сервере ПК требования по предоставлению прав и привилегий по доступу к параметрам настройки программного комплекса исключительно администратору, наделенному соответствующими полномочиями, приведена в пунктах 1.2.1 и 1.2.2.

Критерии оценки:

Результаты проверки считаются положительным, если на сервере ПК выполняется требование по предоставлению прав и привилегий по доступу к параметрам настройки программного комплекса исключительно администратору, наделенному соответствующими полномочиями.

1.2.5 Проверка ограничения неуспешных попыток входа пользователя на сервер ПК

Описание функции:

На сервере ПК реализована автоматическая блокировка возможности авторизации пользователя на сервере ПК с устройства, с которого была осуществлена н четырехкратная неуспешная авторизация пользователя на сервере ПК. Разблокировка такого устройства осуществляется в автоматическом режиме через 15 минут.

Действия:

Последовательность действий по проверке реализации на сервере ПК автоматической блокировки и автоматической разблокировки устройства, с которого были осуществлена четырехкратная неуспешная авторизация пользователя на сервере ПК, приведена в таблице 9.

Таблица 9 – Автоматическая блокировка устройства при неуспешных попытках авторизации с него

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user3** и нажать кнопку ***Подключиться***	Ошибка подключения к серверу ПК
3	Повторить попытки подключения к серверу ПК от имени пользователя **user3** еще три раза	Ошибка подключения к серверу ПК
4	Выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user1**. Указать **верный пароль**	Блокировка возможности подключения к серверу ПК с текущего IP-адреса
5	Через 15 минут выполнить попытку подключения к серверу ПК из окна клиентской консоли от имени и с правами санкционированного пользователя **user1**. Указать **верный пароль**	Открытие клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
6	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих попытки подключения пользователя к серверу ПК и сведения о блокировке и разблокировке устройства

Критерии оценки:

Результаты проверки считаются положительным, если на сервере ПК выполняется автоматическая блокировка устройства, с которого были осуществлена четырехкратная неуспешная авторизация пользователя на сервере ПК. А автоматическая разблокировка такого устройства осуществляется через 15 минут.

1.2.6 Проверка ограничения количества параллельных сеансов доступа для учетной записи пользователя ПК

Описание функции:

На сервере ПК реализовано ограничение числа параллельных (одновременных) сеансов (сессий), основанное на значении идентификатора пользователя программного комплекса. Количество параллельных (одновременных) сеансов (сессий) от имени одной учетной записи пользователя комплекса с разных устройств (средств вычислительной техники) не превышает 16.

Действия:

Последовательность действий по проверке реализации ограничения числа параллельных (одновременных) сеансов (сессий) работы пользователя программного комплекса на сервере ПК приведена в таблице 10.

Таблица 10 – Ограничение количества параллельных сеансов работы пользователя с сервером ПК

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
4	В области *Администрирование* нажать ссылку ***Настройки***, расположенную под кнопкой ***Пользователи***	Открытие окна **«Настройки пользователей»**.
5	В окне **«Настройки пользователей»** отметить параметр ***Ограничение числа разрешенных параллельных сессий для каждого пользователя***,	Успешное изменение параметров безопасности учетных записей пользователей на сервере ПК, возврат во вкладку **Настройки**

№ п/п	Действия	Ожидаемый результат
	ввести в поле ввода значение ***2*** и нажать кнопку ***Сохранить***	
6	Запустить вторую локальную консоль ПК и в окне подключения консоли к серверу ПК ввести логин и пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие второй клиентской консоли ПК
7	Запустить третью локальную консоль ПК и в окне подключения консоли к серверу ПК ввести логин и пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие третьей клиентской консоли ПК, отключение от сервера ПК первой консоли
8	В первой клиентской консоли ввести пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие первой клиентской консоли ПК, отключение от сервера ПК второй консоли
9	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих попытки подключения пользователя к серверу ПК и сведения о принудительном отключении пользователя от работы с сервером ПК

Критерии оценки:

Результаты проверки считаются положительным, если на сервере ПК, в соответствии с установленным значением, выполняется ограничение числа параллельных (одновременных) сеансов (сессий) по работе пользователя с сервером ПК из клиентской консоли.

1.3 Проверка анализа защищенности информации

1.3.1 Проверка выявления, анализа и устранения уязвимостей контролируемого оборудования

Описание функции:

Сервер ПК «Efros Config Inspector» v.3.1 обеспечивает:

– выполнение проверок контролируемых устройств на наличие уязвимостей, связанных с ошибками кода в программном обеспечении, правильностью установки и настройки сетевых устройств и программного обеспечения;

– формирование отчетов, по результатам выполнения проверок устройств на наличие уязвимостей, с описанием выявленных уязвимостей;

– информирование администраторов безопасности о результатах выполнения проверок устройств на наличие уязвимостей;

– информирование администраторов безопасности о способах устранения выявленных уязвимостей.

Действия:

Действия по проверке функций программного комплекса по выявлению, анализу и устранению уязвимостей контролируемого на сервере ПК оборудования приведены в таблице 11.

Таблица 11 – Выявление, анализ и устранение уязвимостей контролируемого оборудования

№ п/п	Действия	Ожидаемый результат
1	Подключение к серверу ПК внешних модулей для отправки сообщений администратору	
1.1	Запустить клиентскую консоль ПК на ЭВМ6	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК в поле ***Сервер*** ввести IP-адрес ЭВМ1, в соответствующие поля ввести логин и пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области *Администрирование* нажать кнопку ***Модули***	Открытие формы управления внешними модулями комплекса
1.5	В форме управления внешними модулями комплекса нажать на ссылку ***Подключить*** для модуля ***Отправка сообщений через MS Exchange***	Открытие окна **«Отправка сообщений через MS Exchange»**
1.6	В окне **«Отправка сообщений через MS Exchange»** заполнить поля ввода: ***Адрес сервера***; ***Отправитель***, ***Имя пользователя*** и ***Пароль***, указав данные пользователя системы MS Exchange, и нажать кнопку ***Применить***	Возврат в форму управления внешними модулями комплекса. Модуль ***Отправка сообщений через MS Exchange*** подключен
1.7	В форме управления внешними модулями комплекса нажать на ссылку ***Подключить*** для модуля ***Отправка писем по протоколу SMTP***	Открытие окна **«Отправка писем по протоколу SMTP»**
1.8	В окне **«Отправка писем по протоколу SMTP»** заполнить поля ввода: ***Адрес сервера***; ***Адрес отправителя*** и ***Пароль отправителя***, указав данные пользователя на сервере SMTP, и нажать кнопку ***Применить***	Возврат в форму управления внешними модулями комплекса. Модуль ***Отправка писем по протоколу SMTP*** подключен
1.9	В форме управления внешними модулями комплекса нажать на ссылку ***Подключить*** для модуля ***Отправка сообщений через MS Lync***	Открытие окна **«Отправка сообщений через MS Lync»**
1.10	В окне **«Отправка сообщений через MS Lync»** заполнить поля ввода: ***Адрес сервера***; ***Адрес***	Возврат в форму управления внешними модулями комплекса. Модуль ***Отправка сообщений через MS Lync*** подключен

№ п/п	Действия	Ожидаемый результат
	отправителя, ***Имя пользователя***, ***Пароль*** и ***Домен***, указав данные пользователя системы MS Lync, и нажать кнопку ***Применить***	
1.11	В форме управления внешними модулями комплекса нажать на ссылку ***Подключить*** для модуля ***Отправка сообщений через MS Lync***	Открытие окна **«Отправка сообщений через MS Lync»**
1.12	В окне **«Отправка сообщений через MS Lync»** заполнить поля ввода: ***Адрес сервера***; ***Адрес отправителя***, ***Имя пользователя***, ***Пароль*** и ***Домен***, указав данные пользователя системы MS Lync, и нажать кнопку ***Применить***	Возврат в форму управления внешними модулями комплекса. Модуль ***Отправка сообщений через MS Lync*** подключен
2	Создание триггера для отправки сообщения администратору безопасности о результатах выполнения проверки контролируемого оборудования на наличие уязвимостей	
2.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
2.2	В области *Настройки контроля* нажать кнопку ***Обработка событий***	Открытие формы настройки обработчиков событий
2.3	В форме настройки обработчиков событий нажать кнопку ***Добавить***	Открытие формы создания обработчика событий
2.4	Во вкладке **Общие** формы создания обработчика событий вести в поле ***Название*** имя создаваемого триггера, отметить параметр ***Активный*** и нажать кнопку ***Сохранить***	Отображение во вкладке **Общие** формы создания обработчика событий введенных данных
2.5	Перейти на вкладку **Условия** формы создания обработчика событий и нажать кнопку ***Добавить***	Появление в рабочей области полей для ввода события и дополнительных условий
2.6	Из раскрывающегося списка поля ***Событие*** выбрать параметр ***Изменение результата проверки*** и нажать ссылку ***Добавить доп.условие***	Открытие окна **«Условие»**
2.7	В раскрывающемся списке поля ввода ***Параметр*** окна **«Условие»** выбрать ***Проверка***	Отображение списка проверок, имеющихся на сервере ПК
2.8	В списке проверок окна **«Условие»** отметить все проверки, которые предназначены для проверки контролируемых устройств на наличие уязвимостей и нажать кнопку ***Сохранить***	Возврат в форму создания обработчика событий, в котором отображены введенные данные
2.9	Нажать ссылку ***Добавить доп.условие***	Открытие окна **«Условие»**
2.10	В раскрывающемся списке поля ввода ***Параметр*** окна **«Условие»** выбрать ***Результат проверки***	Отображение списка возможных результатов проверки

№ п/п	Действия	Ожидаемый результат
2.11	В списке возможных результатов проверки окна **«Условие»** отметить параметры ***Не пройдена*** и ***Пройдена*** и нажать кнопку ***Сохранить***	Возврат в форму создания обработчика событий, в котором отображены введенные данные
2.12	Перейти на вкладку **Действия** формы создания обработчика событий и нажать кнопку ***Добавить***	Появление в рабочей области полей для ввода типа реакции комплекса на событие и параметров его настройки
2.13	Из раскрывающегося списка поля ***Действия*** выбрать параметр ***Отправить сообщение через Exchange***, ввести в поле ввода ***Настройки*** адрес электронной почты администратора безопасности	В форме настройки обработчиков событий отображены введенные данные
2.14	Нажать кнопку ***Добавить*** и из раскрывающегося списка поля ***Действия*** выбрать параметр ***Отправить письмо***, ввести в поле ввода ***Получатели*** адрес электронной почты администратора безопасности	В форме настройки обработчиков событий отображены введенные данные
2.15	Нажать кнопку ***Добавить*** и из раскрывающегося списка поля ***Действия*** выбрать параметр ***Отправить сообщение через Lync***, ввести в поле ввода ***Получатели*** адрес электронной почты администратора безопасности	В форме настройки обработчиков событий отображены введенные данные
2.16	Нажать кнопку ***Добавить*** и из раскрывающегося списка поля ***Действия*** выбрать параметр ***Отправить Syslog сообщение***, ввести в поле ввода ***Адрес Syslog сервера*** IP-адрес сервера сообщений (syslog) и нажать кнопку ***Сохранить***	Возврат в форму настройки обработчиков событий, созданный триггер отображается в списке
3	Выполнение проверок контролируемого оборудования на наличие уязвимостей по протоколу SSH	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
3.2	В панели списка устройств выделить сетевое устройство ***Cisco IOS*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок сетевого устройства ***Cisco IOS***
3.3	В списке проверок сетевого устройства ***Cisco IOS*** выделить проверку ***Уязвимости Cisco IOS***, и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на сетевом устройстве ***Cisco IOS***
3.4	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Уязвимости Cisco IOS***	В рабочей области консоли отобразился отчет с результатами проверки ***Уязвимости Cisco IOS***
3.5	В отчете о выполнении проверки устройства ***Cisco IOS*** на наличие уязвимостей раскрыть выявленную уязвимость и ознакомиться с	Открытие интернет-страницы производителя ПО (cisco.com) с описанием процедуры устранения выявленной уязвимости

№ п/п	Действия	Ожидаемый результат
	информацией по способу устранения выявленной уязвимости, для чего перейти по ссылке на сайт производителя ПО (cisco.com)	
4	Выполнение проверок оборудования на наличие уязвимостей по протоколу Telnet	
4.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
4.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***Huawei VRP***, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства ***Huawei***, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства ***Huawei*** в список контролируемых на сервере ПК
4.3	В панели списка устройств выделить устройство ***Huawei*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Huawei***
4.4	В списке проверок устройства ***Huawei*** выделить проверку ***Уязвимости Huawei*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***Huawei***
4.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Уязвимости Huawei***	В рабочей области консоли отобразился отчет с результатами проверки ***Уязвимости Huawei***
4.6	В отчете о выполнении проверки устройства ***Huawei*** на наличие уязвимостей раскрыть выявленную критичную уязвимость и перейти по ссылке на сайт базы данных уязвимостей ФСТЭК (bdu.fstec.ru)	Открытие интернет-страницы базы данных уязвимостей ФСТЭК России с описанием выявленной уязвимости
4.7	В отчете о выполнении проверки устройства ***Huawei*** на наличие уязвимостей раскрыть выявленную уязвимость и ознакомиться с информацией по способу ее устранения, для чего перейти по ссылке на сайт производителя ПО (huawei.com)	Открытие интернет-страницы производителя ПО (huawei.com) с описанием процедуры устранения выявленную уязвимости
5	Выполнение проверок контролируемого оборудования на наличие уязвимостей по протоколу VIX API	
5.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
5.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***VMware ESXi***, заполнить все поля, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства	Успешное добавление устройства ***VMware ESXi*** в список контролируемых на сервере ПК

№ п/п	Действия	Ожидаемый результат
	VMware ESXi, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	
5.3	В панели списка устройств выделить устройство ***VMware ESXi*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***VMware ESXi***
5.4	В списке проверок устройства ***VMware ESXi*** выделить проверку ***Уязвимости VMware ESXi***, и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***VMware ESXi***
5.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Уязвимости VMware ESXi***	В рабочей области консоли отобразился отчет с результатами проверки ***Уязвимости VMware ESXi***
5.6	В отчете о выполнении проверки устройства ***VMware ESXi*** на наличие уязвимостей раскрыть выявленную уязвимость и перейти по ссылке на сайт базы данных уязвимостей ФСТЭК	Открытие интернет-страницы базы данных уязвимостей ФСТЭК России с описанием выявленной уязвимости
5.7	В отчете о выполнении проверки устройства ***VMware ESXi*** на наличие уязвимостей раскрыть выявленную уязвимость и ознакомиться с информацией по способу устранения выявленной уязвимости, для чего перейти по ссылке на сайт производителя ПО (vmware.com)	Открытие интернет-страницы производителя ПО (vmware.com) с описанием процедуры устранения выявленной уязвимости
6	Выполнение проверок оборудования по протоколу CPMI	
6.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
6.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***Check Point SmartCenter***, заполнить все поля, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства ***Check Point SmartCenter***, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства ***Check Point SmartCenter*** в список контролируемых на сервере ПК
6.3	В панели списка устройств выделить устройство ***Check Point SmartCenter*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Check Point SmartCenter***
6.4	В списке проверок устройства ***Check Point SmartCenter*** выделить проверку ***Check Point SmartCenter Rule Policies***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***Check Point SmartCenter***

№ п/п	Действия	Ожидаемый результат
	Firewall Compliance, и нажать кнопку ***Обновить***	
6.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Check Point SmartCenter Rule Policies Firewall Compliance***	В рабочей области консоли отобразился отчет с результатами проверки ***Check Point SmartCenter Rule Policies Firewall Compliance***
7	Выполнение проверок оборудования на наличие уязвимостей по протоколу REST	
7.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
7.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***Cisco ACS***, заполнить все поля, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства ***Cisco ACS***, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства ***Cisco ACS*** в список контролируемых на сервере ПК
7.3	В панели списка устройств выделить устройство ***Cisco ACS*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Cisco ACS***
7.4	В списке проверок устройства ***Cisco ACS*** выделить проверку ***Уязвимости Cisco ACS***, и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***Cisco ACS***
7.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Уязвимости Cisco ACS***	В рабочей области консоли отобразился отчет с результатами проверки ***Уязвимости Cisco ACS***
7.6	В отчете о выполнении проверки устройства ***Cisco ACS*** на наличие уязвимостей раскрыть выявленную уязвимость и перейти по ссылке на сайт базы данных уязвимостей ФСТЭК (bdu.fstec.ru)	Открытие интернет-страницы базы данных уязвимостей ФСТЭК России с описанием выявленной уязвимости
7.7	В отчете о выполнении проверки устройства ***Cisco ACS*** на наличие уязвимостей раскрыть выявленную уязвимость и ознакомиться с информацией по способу устранения выявленной уязвимости, для чего перейти по ссылке на сайт производителя ПО (cisco.com)	Открытие интернет-страницы производителя ПО (cisco.com) с описанием процедуры устранения выявленной уязвимости
8	Выполнение проверок оборудования на наличие уязвимостей по протоколу Cisco Administrative XML (AXL)	
8.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**

№ п/п	Действия	Ожидаемый результат
8.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***Cisco UCM***, заполнить все поля, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства ***Cisco UCM***, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства ***Cisco UCM*** в список контролируемых на сервере ПК
8.3	В панели списка устройств выделить устройство ***Cisco UCM*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Cisco UCM***
8.4	В списке проверок устройства ***Cisco UCM*** выделить проверку ***Уязвимости Cisco UCM***, и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***Cisco UCM***
8.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Уязвимости Cisco UCM***	В рабочей области консоли отобразился отчет с результатами проверки ***Уязвимости Cisco UCM***
8.6	В отчете о выполнении проверки устройства ***Cisco UCM*** на наличие уязвимостей раскрыть выявленную уязвимость и перейти по ссылке на сайт базы данных уязвимостей ФСТЭК (bdu.fstec.ru)	Открытие интернет-страницы базы данных уязвимостей ФСТЭК России с описанием выявленной уязвимости
8.7	В отчете о выполнении проверки устройства ***Cisco UCM*** на наличие уязвимостей раскрыть выявленную уязвимость и ознакомиться с информацией по способу устранения выявленной уязвимости, для чего перейти по ссылке на сайт производителя ПО (cisco.com)	Открытие интернет-страницы производителя ПО (cisco.com) с описанием процедуры устранения выявленной уязвимости
9	Выполнение проверок оборудования по протоколу WMI	
9.1	В локальной консоли перейти в раздел ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
9.2	В окне **«Новое устройство»** из выпадающего списка поля ***Тип*** выбрать параметр ***Standalone Hyper-V 2008R2***, заполнить все поля, определяющие параметры добавляемого на сервер ПК устройства, ввести идентификационные данные учетной записи пользователя для авторизации на устройстве и нажать кнопку ***Добавить***	Успешное добавление устройства ***Standalone Hyper-V 2008R2*** в список контролируемых на сервере ПК

№ п/п	Действия	Ожидаемый результат
9.3	В панели списка устройств выделить устройство ***Hyper-V*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Hyper-V***
9.4	В списке проверок устройства ***Hyper-V*** выделить проверку HyperV Best Practices Analyzer Compliance и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки на устройстве ***Hyper-V***
9.5	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***HyperV Security guide***	В рабочей области консоли отобразился отчет с результатами проверки ***HyperV Security guide***
10	Просмотр результатов информирования администратора безопасности о результатах выполнения проверок устройств на наличие уязвимостей	
10.1	На рабочей станции ЭВМ6 запустить MS Outlook и просмотреть сообщения, полученные от пользователя, указанного в п. 1.6 и п. 1.8	В сообщениях содержится информация о результатах проверок устройств на наличие уязвимостей
10.2	На ЭВМ1 просмотреть полученные с сервера ПК syslog-сообщения	В сообщениях содержится информация о результатах проверок устройств на наличие уязвимостей
10.3	На рабочей станции ЭВМ6 просмотреть сообщения, полученные по протоколу Microsoft RTC API (MS Lync)	В сообщениях содержится информация о результатах проверок устройств на наличие уязвимостей
11	Просмотр списка событий в локальной консоли ПК	
11.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о выполнении проверок контролируемых устройств, выполнении триггера и результатах выполнения проверок.
12	Повторить действия, изложенные в пунктах 1-11 на ЭВМ1-ЭВМ6 для остальных операционных систем	Повторение полученных результатов

Критерии оценки:

Результаты проверки считаются положительными, если на сервере ПК обеспечивается:

– выполнение проверок контролируемых устройств на наличие уязвимостей, связанных с ошибками кода в программном обеспечении, правильностью установки и настройки сетевых устройств и программного обеспечения;

– формирование отчетов, по результатам выполнения проверок устройств на наличие уязвимостей, с описанием выявленных уязвимостей;

– информирование администраторов безопасности о результатах выполнения проверок устройств на наличие уязвимостей;

– информирование администраторов безопасности о способах устранения выявленных уязвимостей.

1.3.2 Проверка контроля установки обновлений программного обеспечения на контролируемом на сервере ПК оборудовании

Описание функции:

Программный комплекс обеспечивает контроль установки обновлений общесистемного, прикладного и специального программного (микропрограммного) обеспечения контролируемого на сервере ПК оборудования.

На сервере ПК реализована возможность определения периодичности выполнения проверок, установленных на контролируемом оборудовании обновлений прикладного и специального программного (микропрограммного) обеспечения.

Действия:

Действия по проверке функций программного комплекса по контролю установки обновлений программного обеспечения на контролируемом на сервере ПК оборудовании приведены в таблице 12.

Таблица 12 – Контроль установки обновлений программного обеспечения на контролируемом оборудовании

№ п/п	Действия	Ожидаемый результат
1	Создание триггера для отправки сообщения администратору безопасности о нарушении целостности отчета	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области *Настройки сервера* нажать кнопку ***Обработка событий***	Открытие формы настройки обработчиков событий
1.5	В форме настройки обработчиков событий нажать кнопку ***Добавить***	Открытие формы создания обработчика событий
1.6	Во вкладке **Общие** формы создания обработчика событий вести в поле ***Название*** имя создаваемого триггера, отметить параметр ***Активный*** и нажать кнопку ***Сохранить***	Отображение во вкладке **Общие** формы создания обработчика событий введенных данных
1.7	Перейти на вкладку **Условия** формы создания обработчика событий и нажать кнопку ***Добавить***	Появление в рабочей области полей для ввода события и дополнительных условий
1.8	Из раскрывающегося списка поля ***Событие*** выбрать параметр ***Нарушение целостности***	Во вкладке **Условие** отображены введенные данные

№ п/п	Действия	Ожидаемый результат
1.9	Перейти на вкладку **Действия** формы создания обработчика событий и нажать кнопку ***Добавить***	Появление в рабочей области полей для ввода типа реакции комплекса на событие и параметров его настройки
1.10	Из раскрывающегося списка поля ***Действия*** выбрать параметр ***Отправить сообщение через Exchange***, ввести в поле ввода ***Настройки*** адрес электронной почты администратора безопасности и нажать кнопку ***Сохранить***	Возврат в форму настройки обработчиков событий, созданный триггер отображается в списке.
2	Проверка установленного программного обеспечения на рабочих станциях и серверах с ОС Windows	
2.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
2.2	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
2.3	В окне **«Новое устройство»** выбрать из выпадающего поля ***Тип*** параметр ***Windows***, заполнить все поля, определяющие параметры добавляемой на сервер ПК рабочей станции ***Console*** и нажать кнопку ***Добавить***	Успешное добавление рабочей станции ***Console*** в список контролируемых на сервере ПК
2.4	В панели списка устройств выделить рабочую станцию ***Console*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов, загружаемых с рабочей станции ***Console***
2.5	Во вкладке **Отчеты** выделить отчет ***Программы и обновления*** и нажать кнопку ***Настройки***	Открытие окна настройки параметров загрузки отчета ***Программы и обновления***
2.6	В окне настройки параметров загрузки отчета ***Программы и обновления*** из выпадающего списка поля ***Использование*** выбрать параметр ***Контроль изменений*** и нажать кнопку ***Применить***	Возврат во вкладку **Отчеты**, в поле ***Состояние*** отчета ***Программы и обновления*** отображено значение ***Контроль изменений***
2.7	Во вкладке **Отчеты** выделить отчет ***Программы и обновления*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Программы и обновления*** с рабочей станции ***Console***
2.8	На рабочей станции ***Console*** удалить установленную программу	Программа удалена с рабочей станции
2.9	В панели списка устройств выделить рабочую станцию ***Console*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов, загружаемых с рабочей станции ***Console***
2.10	Во вкладке **Отчеты** выделить отчет ***Программы и обновления*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Программы и обновления*** с рабочей станции ***Console***. По окончании загрузки появляется уведомление о нарушении целостности отчета.

№ п/п	Действия	Ожидаемый результат
2.11	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***Программы и обновления***	В рабочей области консоли открылась форма просмотра отчета ***Программы и обновления*** об установленных на рабочей станции ***Console*** программном обеспечении и обновлениях ОС
2.12	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
2.13	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять***	В форме сравнения отчетов пропала кнопка ***Принять***
2.14	Последовательно закрыть формы сравнения и просмотра отчета	Возврат во вкладку **Отчеты** рабочей станции ***Console***
3	**Проверка выполнения загрузки отчетов с контролируемого оборудования по расписанию**	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
3.2	В области *Настройки сервера* нажать кнопку ***Расписания***	Открытие формы управления расписаниями программного комплекса
3.3	В форме управления расписаниями программного комплекса нажать кнопку ***Добавить***	Открытие окна **«Новое расписание»**
3.4	В окне **«Новое расписание»**: - ввести имя расписания в поле ***Название***; - отметить параметр ***Активно***; - в поле ***Периодичность*** установить значение ***Минуты***; - в поле ***Каждые*** установить значение ***5*** минут; - в поле ***Действие*** выбрать значение ***Загрузка отчётов***; - нажать кнопку ***Сохранить***	Возврат в форму управления расписаниями программного комплекса, в списке отображается созданное расписание
3.5	В форме управления расписаниями программного комплекса нажать ссылку ***для устройств***, расположенную под названием расписания	Открытие окна настройки использования расписания для контролируемых на сервере ПК устройств
3.6	В окне настройки использования расписания для контролируемых на сервере ПК устройств разрешить использование этого расписания для рабочей станции ***Console***, для остальных устройств – ***запретить***, установив соответствующее значение в поле ***Использование*** и нажать кнопку ***Сохранить***	Введенные параметры использования расписания сохранены, осуществлен возврат в форму управления расписаниями программного комплекса
3.7	На рабочей станции ***Console*** удалить установленное обновление	Обновление удалено с рабочей станции. При автоматической загрузке отчетов с рабочей станции ***Console*** появляется уведомление о нарушении целостности отчета ***Программы и обновления***

№ п/п	Действия	Ожидаемый результат
3.8	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***Программы и обновления***	В рабочей области консоли форма просмотра отчета об установленных на рабочей станции ***Console*** программном обеспечении и обновлениях ОС
3.9	В форме просмотра отчета нажать кнопку ***Сравнить***	Открытие окна **«Выбрать отчет для сравнения»**
3.10	В окне **«Выбрать отчет для сравнения»** сделать двойной щелчок кнопкой мыши на эталонном отчете ***Программы и обновления***	Открытие формы сравнения текущего отчета с эталонным
3.11	Ознакомиться с результатами сравнения отчетов	В форме сравнения отчетов отображены изменения в составе программного обеспечения рабочей станции ***Console***
4	Просмотр результатов информирования администратора безопасности о результатах выполнения проверок устройств на наличие уязвимостей	
4.1	На рабочей станции ***Console*** запустить MS Outlook	Открытие окна MS Outlook
4.2	Просмотреть сообщения, полученные от пользователя, указанного в п. 1.10	В сообщениях содержится информация о результатах проверок устройств на наличие уязвимостей и нарушениях целостности отчета
5	Просмотр списка событий в локальной консоли программного комплекса	
5.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов контролируемых устройств, выполнении триггера и нарушениях целостности контролируемых отчетов.

Критерии оценки:

Результаты проверки считаются положительными, если:

– программный комплекс обеспечивает контроль установки обновлений общесистемного, прикладного и специального программного (микропрограммного) обеспечения контролируемого на сервере ПК оборудования;

– на сервере ПК реализована возможность определения периодичности выполнения проверок, установленных на контролируемом оборудовании обновлений прикладного и специального программного (микропрограммного) обеспечения.

1.3.3 Проверка контроля работоспособности, параметров настройки и правильности функционирования программного обеспечения контролируемого оборудования

Описание функции:

Программный комплекс выполняет проверки соответствия конфигурации контролируемых устройств требованиям безопасности (compliance проверки) и обеспечивает инвентаризацию параметров настройки программного обеспечения и конфигурации контролируемого на сервере ПК оборудования;

При выполнении инвентаризации параметров настройки программного обеспечения и конфигурации программный комплекс позволяет выполнить следующие операции:

– установку эталонной версии отчета о конфигурации оборудования;
– ведение истории загруженных версий отчетов;
– сравнение текстов загруженных версий отчетов;
– экспорт загруженной версии отчета в файл.

Действия:

Действия по проверке функций программного комплекса по контролю работоспособности, параметров настройки и правильности функционирования программного обеспечения на контролируемом на сервере ПК оборудовании приведены в таблице 13.

Таблица 13 – Контроль работоспособности, параметров настройки и правильности функционирования ПО оборудования

№ п/п	Действия	Ожидаемый результат
1	Контроль конфигурационных файлов	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
1.4	В панели списка устройств выделить сетевое устройство ***Cisco IOS*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок сетевого устройства ***Cisco IOS***
1.5	Во вкладке **Отчеты** выделить отчет ***Cisco IOS 'show running'*** и, вызвав контекстное меню выделенного отчета, выбрать пункт ***Настройка отчета***	Открытие окна настройки параметров загрузки отчета ***Cisco IOS 'show running'***
1.6	В окне настройки параметров загрузки отчета ***Cisco IOS 'show running'*** из выпадающего списка поля ***Использование*** выбрать параметр ***Контроль изменений*** и нажать кнопку ***Применить***	Возврат во вкладку **Отчеты**, в поле ***Состояние*** отчета ***Cisco IOS 'show running'*** отображено значение ***Контроль изменений***
1.7	Штатными средствами управления устройства ***Cisco IOS*** изменить его рабочую (*running*) конфигурацию	Рабочая конфигурация сетевого устройства ***Cisco IOS*** изменена
1.8	В клиентской консоли во вкладке **Отчеты** выделить отчет ***Cisco IOS***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Cisco IOS 'show running'*** с сетевого устройства ***Cisco IOS***.

№ п/п	Действия	Ожидаемый результат
	'show running' и нажать кнопку ***Обновить***	По окончании загрузки появляется уведомление о нарушении целостности отчета.
1.9	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***Cisco IOS 'show running'***	В рабочей области консоли открылась форма просмотра отчета ***Cisco IOS 'show running'***
1.10	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**
1.11	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержится отчет о конфигурации ***show running*** устройства ***Cisco IOS***
1.12	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
1.13	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять***	В форме сравнения отчетов пропала кнопка ***Принять текущую версию за эталон***
1.14	Последовательно закрыть формы сравнения и просмотра отчета	Возврат во вкладку **Отчеты** сетевого устройства ***Cisco IOS***
2	Проверка соответствия конфигурации контролируемых устройств требованиям безопасности	
2.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
2.2	В панели списка устройств выделить сетевое устройство ***Cisco IOS*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок сетевого устройства ***Cisco IOS***
2.3	Во вкладке **Отчеты** выделить проверку ***Проверка политик CIS для Cisco IOS*** нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки ***Проверка политик CIS для Cisco IOS***
2.4	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Проверка политик CIS для Cisco IOS***	В рабочей области консоли открылась форма просмотра результатов проверки ***Проверка политик CIS для Cisco IOS***
2.5	В форме просмотра результатов проверки ***Проверка политик CIS для Cisco IOS*** отметить параметр ***Только нарушения*** и ознакомиться с выявленными нарушениями требований безопасности	В форме просмотра результатов проверки ***Проверка политик CIS для Cisco IOS*** в списке выполненных правил отображаются только нарушения требований безопасности
2.6	Штатными средствами управления устройства ***Cisco IOS*** устранить одно из выявленных нарушений требований безопасности	В конфигурацию сетевого устройства ***Cisco IOS*** внесены изменения
2.7	В клиентской консоли во вкладке **Отчеты** выделить проверку ***Проверка политик CIS для Cisco IOS*** нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса выполнения проверки ***Проверка политик CIS для Cisco IOS***
2.8	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на проверке ***Проверка политик CIS для Cisco IOS***	В рабочей области консоли открылась форма просмотра результатов проверки ***Проверка политик CIS для Cisco IOS***

№ п/п	Действия	Ожидаемый результат
2.9	В форме просмотра результатов проверки ***Проверка политик CIS для Cisco IOS*** отметить параметр ***Только нарушения*** и ознакомиться с выявленными нарушениями требований безопасности	Устраненное в п. 2.7 нарушение отсутствует в списке выявленных нарушений требований безопасности
2.10	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**
2.11	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержатся результаты выполнения проверки соответствия конфигурации устройства ***Cisco IOS*** требованиям безопасности
3	Просмотр архива версий загруженных отчетов о конфигурации оборудования и выполнении проверок	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
3.2	В панели списка устройств выделить сетевое устройство ***Cisco IOS*** и в рабочей области перейти на вкладку **Архив**	Во вкладке **Архив** рабочей области отобразился список проверок сетевого устройства ***Cisco IOS***, и отчетов, в настройках использования которых установлен параметр ***Архив версий*** или ***Контроль целостности***
3.3	Во вкладке **Архив** выполнить двойной щелчок левой кнопкой мыши на строке с текущей версии отчета ***Cisco IOS 'show running'***	В рабочей области консоли открылась форма просмотра отчета ***Cisco IOS 'show running'***
3.4	В форме просмотра отчета ***Cisco IOS 'show running'*** перейти на вкладку ***История изменений***	Во вкладке ***История изменений*** отображается список изменений в хранящихся в базе данных комплекса версиях отчета ***Cisco IOS 'show running'***
3.5	В форме просмотра отчета ***Cisco IOS 'show running'*** перейти на вкладку ***Просмотр*** и нажать кнопку ***Сравнить***	Открытие окна выбора версии отчета для сравнения
3.6	В окне выбора версии отчета для сравнения выполнить двойной щелчок левой кнопкой мыши на строке с первой версией отчета ***Cisco IOS 'show running'***	Открытие формы сравнения версий отчета, в которой удаленные параметры отображаются на красном фоне, добавленные – на зеленом
3.7	Закрыть формы просмотра и сравнения отчетов	Возврат во вкладку **Архив** устройства ***Cisco IOS***
4	Просмотр списка событий в локальной консоли программного комплекса	
4.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов и выполнении проверок контролируемых устройств.

Критерии оценки:

Результаты проверки считаются положительными, если программный комплекс:

– выполняет проверки соответствия конфигурации контролируемых устройств требованиям безопасности;

– обеспечивает инвентаризацию параметров настройки программного обеспечения и конфигурации контролируемого на сервере ПК оборудования;

При выполнении инвентаризации параметров настройки программного обеспечения и конфигурации программный комплекс выполняются следующие операции:

– установка эталонной версии отчета о конфигурации оборудования;

– просмотр истории загруженных версий отчетов;

– сравнение текстов загруженных версий отчетов;

– экспорт загруженной версии отчета в файл.

1.3.4 Проверка выполнения контроля состава технических средств и программного обеспечения контролируемого оборудования

Описание функции:

Программный комплекс осуществляет:

– контроль состава программного обеспечения и настроек конфигурации контролируемого оборудования;

– обнаружение изменений программного обеспечения и настроек конфигурации контролируемого оборудования;

– контроль состава программного обеспечения и конфигурационных настроек контролируемого оборудования по расписанию;

– оповещение администратора при обнаружении изменений программного обеспечения и настроек конфигурации контролируемого оборудования.

Действия:

Действия по проверке функций программного комплекса по контролю состава технических средств и программного обеспечения контролируемого на сервере ПК оборудования приведены в пунктах 1.3.2 и 1.3.3.

Критерии оценки:

Результаты проверки считаются положительными, если программный комплекс осуществляет:

– контроль состава программного обеспечения и настроек конфигурации контролируемого оборудования;

– обнаружение изменений программного обеспечения и настроек конфигурации контролируемого оборудования;

– контроль состава программного обеспечения и конфигурационных настроек контролируемого оборудования по расписанию;

– оповещение администратора при обнаружении изменений программного обеспечения и настроек конфигурации контролируемого оборудования.

1.3.5 Проверка выполнения контроля правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей программного комплекса

Описание функции:

Программный комплекс осуществляет:

– контроль правил генерации и смены паролей пользователей ПК по параметрам:

– минимальная сложность пароля;

– максимальное и минимальное время действия пароля,

– запрет использования любого из предыдущих паролей;

– контроль реализации правил разграничения доступом пользователей комплекса к контролируемому оборудованию;

– контроль реализации полномочий (ролей) пользователей ПК при работе с комплексом;

– регистрацию событий, связанных со сменой паролей пользователей ПК, заведением и удалением учетных записей пользователей ПК, изменением правил разграничения доступом и полномочий пользователей ПК.

Действия:

Действия по проверке функций программного комплекса по осуществлению контроля правил генерации и смены паролей пользователей ПК, заведения и удаления учетных записей пользователей комплекса, реализации правил разграничения доступом, полномочий пользователей программного комплекса приведены в пунктах 1.1.4, 1.2.2 и 1.2.3.

Критерии оценки:

Результаты проверки считаются положительными, если программный комплекс осуществляет:

а) контроль правил генерации и смены паролей пользователей ПК по параметрам:
- минимальная сложность пароля;
- максимальное и минимальное время действия пароля,
- запрет использования любого из предыдущих паролей;

б) контроль реализации правил разграничения доступом пользователей комплекса к контролируемому оборудованию;

в) контроль реализации полномочий (ролей) пользователей ПК при работе с комплексом;
г) регистрацию событий, связанных со сменой паролей пользователей ПК, заведением и удалением учетных записей пользователей ПК, изменением правил разграничения доступом и полномочий пользователей ПК.

1.4 Проверка выполнения контроля целостности программного обеспечения контролируемого на сервере ПК оборудования

Описание функции:

Программный комплекс обеспечивает выполнение следующих функций:

– контроль целостности программного обеспечения контролируемого оборудования, включая их обновления, по контрольным суммам компонентов программного обеспечения в процессе загрузки отчетов о конфигурации оборудования;

– осуществление контроля целостности программного обеспечения контролируемого оборудования по расписанию;

– оповещение администраторов при обнаружении изменений программного обеспечения контролируемого оборудования.

Действия:

Действия по проверке функций программного комплекса по выполнению контроля целостности программного обеспечения контролируемого на сервере ПК оборудования приведены в таблице 14.

Таблица 14 – Контроль целостности программного обеспечения оборудования

№ п/п	Действия	Ожидаемый результат
1	Создание пользовательского отчета по контролю целостности программного обеспечения ОС Windows	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи существующего на сервере ПК пользователя **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК
1.4	В области *Настройки контроля* нажать кнопку ***Отчеты***	Открытие формы создания и настройки использования отчетов, предназначенных для загрузки с контролируемых устройств
1.5	В форме настройки отчетов нажать кнопку ***Добавить***	Открытие окна **«Новый отчет»**

№ п/п	Действия	Ожидаемый результат
1.6	В окне **«Новый отчет»** ввести имя отчета: ***Windows CI***, список масок контролируемых файлов, список масок файлов, исключаемых с контроля, отметить параметры ***Разрешить использование*** и ***Включить контроль целостности*** и нажать кнопку ***Применить***	Успешное добавление нового отчета, возврат в форму создания и настройки использования отчетов
2	Создание пользовательского отчета по контролю целостности программного обеспечения ОС Linux	
2.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК
2.2	В области *Настройки сервера* нажать кнопку ***Отчеты***	Открытие формы создания и настройки использования отчетов, предназначенных для загрузки с контролируемых устройств
2.3	В форме настройки отчетов нажать кнопку ***Добавить***	Открытие окна **«Новый отчет»**
2.4	В окне **«Новый отчет «Linux файлы»** выделить параметр ***Linux файлы,*** ввести имя отчета: ***Linux CI***, список масок контролируемых файлов, список масок файлов, исключаемых с контроля, отметить параметры ***Разрешить использование*** и ***Включить контроль целостности*** и нажать кнопку ***Применить***	Успешное добавление нового отчета, возврат в форму создания и настройки использования отчетов
3	Выполнение проверки контроля целостности программного обеспечения ОС Windows	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
3.2	В панели списка устройств выделить локальную рабочую станцию ***Console*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок рабочей станции ***Console***
3.3	Во вкладке **Отчеты** выделить отчет ***Windows CI*** и, вызвав контекстное меню выделенного отчета, выбрать пункт ***Обновить отчет***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Windows CI*** с рабочей станции ***Console***
3.4	На локальной рабочей станции ***Console*** изменить контролируемый на сервере ПК файл	Файл изменен
3.5	В клиентской консоли во вкладке **Отчеты** выделить отчет ***Windows CI*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Windows CI*** с рабочей станции ***Console***. По окончании загрузки появляется уведомление о нарушении целостности отчета.
3.6	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***Windows CI***	В рабочей области консоли открылась форма просмотра отчета ***Windows CI***
3.7	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**

№ п/п	Действия	Ожидаемый результат
3.8	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержится отчет о результатах проверки целостности контролируемых на рабочей станции ***Console*** файлах
3.9	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
3.10	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять***	В форме сравнения отчетов пропала кнопка ***Принять***
4	Выполнение проверки контроля целостности программного обеспечения ОС Linux	
4.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
4.2	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
4.3	В окне **«Новое устройство»**: - в поле ***Имя*** ввести значение ***Linux***, - выбрать из выпадающего поля ***Тип*** параметр ***Linux***, - заполнить все поля, определяющие параметры добавляемого на сервер ПК оборудования под управлением ОС Linux (***IP-адрес***, ***имя*** и ***пароль пользователя***, ***порт SSH***), - нажать кнопку ***Добавить***	Успешное добавление оборудования под управлением ОС Linux в список контролируемых на сервере ПК
4.4	В панели списка устройств выделить устройство ***Linux*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок устройства ***Linux***
4.5	Во вкладке **Отчеты** выделить отчет устройство ***Linux CI*** и, вызвав контекстное меню выделенного отчета, выбрать пункт ***Обновить отчет***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Linux CI*** с устройства ***Linux***
4.6	На устройстве ***Linux*** штатными средствами изменить контролируемый на сервере ПК файл	Файл изменен
4.7	В клиентской консоли во вкладке **Отчеты** выделить отчет ***Linux CI*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***Linux CI*** с устройства ***Linux***. По окончании загрузки появляется уведомление о нарушении целостности отчета.
4.8	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***Linux CI***	В рабочей области консоли открылась форма просмотра отчета ***Linux CI***
4.9	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**
4.10	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержится отчет о результатах проверки целостности контролируемых на устройстве ***Linux*** файлах

№ п/п	Действия	Ожидаемый результат
4.11	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
4.12	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять текущую версию за эталон***	В форме сравнения отчетов пропала кнопка ***Принять текущую версию за эталон***
5	Просмотр результатов информирования администратора безопасности о результатах выполнения проверок устройств на наличие уязвимостей	
5.1	На рабочей станции ***Console*** запустить MS Outlook	Открытие окна MS Outlook
5.2	Просмотреть сообщения, полученные от пользователя, указанного в обработчике события нарушения целостности отчета	В сообщениях содержится информация о нарушениях целостности отчета
6	Просмотр списка событий в локальной консоли программного комплекса	
6.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов, выполнении триггеров и сообщения о нарушении целостности загруженных отчетов

Критерии оценки:

Результаты проверки считаются положительными, если программный комплекс выполняет:

– контроль целостности программного обеспечения контролируемого оборудования, включая их обновления, по контрольным суммам компонентов программного обеспечения в процессе загрузки отчетов о конфигурации оборудования;

– осуществление контроля целостности программного обеспечения контролируемого оборудования по расписанию;

– оповещение администраторов при обнаружении изменений программного обеспечения контролируемого оборудования.

1.5 Проверка выполнения контроля целостности виртуальной инфраструктуры и ее конфигураций

Описание функции:

Программный комплекс в целях обеспечения контроля целостности виртуальной инфраструктуры и ее конфигураций обеспечивает выполнение следующих функций:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем;

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем);

– контроль целостности резервных копий виртуальных машин (контейнеров);

– контроль состава аппаратной части компонентов виртуальной инфраструктуры.

Действия:

Действия по проверке функций программного комплекса по выполнению контроля целостности виртуальной инфраструктуры и ее конфигураций приведены в таблице 15.

Таблица 15 – Контроль целостности виртуальной инфраструктуры и ее конфигураций

№ п/п	Действия	Ожидаемый результат
1	Контроль конфигураций виртуальной инфраструктуры	
1.1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
1.2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи существующего на сервере ПК пользователя **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
1.3	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
1.4	В окне **«Новое устройство»**: - в поле ***Имя*** ввести значение ***vCenter Windows,*** - выбрать из выпадающего поля ***Тип*** параметр ***vCenter***, - заполнить все поля, определяющие параметры добавляемого на сервер ПК сервера управления VMware vSphere (***IP-адрес***, ***имя*** и ***пароль пользователя***), - нажать кнопку ***Добавить***	Успешное добавление сервера управления VMware vSphere в список контролируемых на сервере ПК
1.5	В панели списка устройств выделить сервер управления ***VMware vCenter*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и сервера управления ***VMware vCenter***
1.6	Во вкладке **Отчеты** выделить отчет ***VMware vSphere Дерево иерархии*** и, вызвав контекстное меню выделенного отчета, выбрать пункт ***Настройка отчета***	Открытие окна настройки параметров загрузки отчета ***Cisco IOS 'show running'***
1.7	В окне настройки параметров загрузки отчета ***VMware vSphere Дерево***	Возврат во вкладку **Отчеты**, в поле ***Состояние*** отчета ***VMware vSphere***

№ п/п	Действия	Ожидаемый результат
	иерархии из выпадающего списка поля ***Использование*** выбрать параметр ***Контроль изменений*** и нажать кнопку ***Применить***	***Дерево иерархии*** отображено значение ***Контроль изменений***
1.8	Повторить действия пунктов 1.6 и 1.7 по установке эталонной версии для отчета ***VMware vSphere Роли пользователей***	В поле ***Состояние*** отчета ***VMware vSphere Роли пользователей*** отображено значение ***Контроль изменений***
1.9	Перейти на вкладку **Архив** и просмотреть наличие эталонных версии отчетов ***VMware vSphere Дерево иерархии*** и ***VMware vSphere Роли пользователей***	Наличие сведений о дате и времени принятия эталонных версий отчетов во вкладке **Архив**
1.10	Средствами управления VMware vSphere внести изменения в конфигурацию виртуальной инфраструктуры	Изменения внесены
1.11	В клиентской консоли комплекса перейти во вкладку **Статус** сервера управления ***VMware vCenter*** и в области *Действия с устройством* нажать кнопку ***Загрузить***	Выполняется загрузка отчетов ***VMware vSphere Дерево иерархии*** и ***VMware vSphere Роли пользователей***. По окончании загрузки появляется уведомление о нарушении целостности отчета.
1.12	Перейти во вкладку **Отчеты** и выполнить двойной щелчок левой кнопкой мыши на отчете ***VMware vSphere Дерево иерархии***	В рабочей области консоли открылась форма просмотра отчета ***VMware vSphere Дерево иерархии***
1.13	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
1.14	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять текущую версию за эталон***	В форме сравнения отчетов пропала кнопка ***Принять текущую версию за эталон***
1.15	Перейти во вкладку **Архив**	Наличие нескольких версий отчета конфигурации виртуальной инфраструктуры
1.16	Выполнить двойной щелчок левой кнопкой мыши на одной из версий отчета ***VMware vSphere Роли пользователей***	В рабочей области консоли открылась форма просмотра отчета ***VMware vSphere Дерево иерархии***
1.17	В форме просмотра отчета нажать на кнопку ***Экспорт*** и выбрать пункт меню ***Xml***	Открытие окна **«Сохранить как»**
1.18	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержатся данные отчета ***VMware vSphere Дерево иерархии***
1.19	Повторить действия пунктов 1.16 – 1.18 для отчета ***VMware vSphere Роли пользователей***	Сохранен файл, в котором содержатся данные отчета ***VMware vSphere Роли пользователей***
2	Создание пользовательского отчета по контролю целостности программного обеспечения гипервизоров VMware ESXi	
2.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **Настройка**	В рабочей области консоли отобразился список параметров сервера ПК

№ п/п	Действия	Ожидаемый результат
2.2	В области *Настройки сервера* нажать кнопку ***Отчеты***	Открытие формы создания и настройки использования отчетов, предназначенных для загрузки с контролируемых устройств
2.3	В форме настройки отчетов нажать кнопку ***Добавить***	Открытие окна **«Пользовательские отчеты»**
2.4	В окне **«Пользовательские отчеты»** выделить параметр ***VMware ESXi файлы*** и нажать кнопку ***Далее***	Открытие окна **«Новый отчет «*VMware ESXi* файлы»**
2.5	В окне **«Новый отчет «Linux файлы»** ввести имя отчета: ***VMware CI***, список масок контролируемых файлов, список масок файлов, исключаемых с контроля, отметить параметр ***Выполнение команд от root*** и нажать кнопку ***Далее***	Открытие окна **«Настройки использования»**
2.6	В окне **«Настройки использования»** отметить параметры ***Разрешить использование*** и ***Включить контроль целостности*** и нажать кнопку ***Применить***	Успешное добавление нового отчета, возврат в форму создания и настройки использования отчетов
3	Выполнение проверки контроля целостности программного обеспечения на гипервизоре VMware ESXi	
3.1	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
3.2	В локальной консоли перейти на вкладку ***Устройства*** и нажать кнопку ***Добавить устройство***	Открытие окна **«Новое устройство»**
3.3	В окне **«Новое устройство»**: - в поле ***Имя*** ввести значение ***VMware ESXi***, - выбрать из выпадающего поля ***Тип*** параметр ***VMware ESXi***, - заполнить все поля, определяющие параметры добавляемого на сервер ПК гипервизора VMware ESXi (***IP-адрес***, ***имя*** и ***пароль пользователя***, ***порт SSH***), - нажать кнопку ***Добавить***	Успешное добавление гипервизора VMware ESXi в список контролируемых на сервере ПК
3.4	В панели списка устройств выделить гипервизор ***VMware ESXi*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список отчетов и проверок гипервизора ***VMware ESXi***
3.5	Во вкладке **Отчеты** выделить отчет устройство ***VMware CI*** и, вызвав контекстное меню выделенного отчета, выбрать пункт ***Обновить отчет***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***VMware CI*** с гипервизора ***VMware ESXi***
3.6	На гипервизоре ***VMware ESXi*** штатными средствами изменить контролируемый на сервере ПК файл	Файл изменен
3.7	В клиентской консоли во вкладке **Отчеты** выделить отчет ***VMware CI*** и нажать кнопку ***Обновить***	Во вкладке **Отчеты** отображается ход процесса загрузки отчета ***VMware CI*** с гипервизора ***VMware ESXi***. По окончании

№ п/п	Действия	Ожидаемый результат
		загрузки появляется уведомление о нарушении целостности отчета.
3.8	Во вкладке **Отчеты** выполнить двойной щелчок левой кнопкой мыши на отчете ***VMware CI***	В рабочей области консоли открылась форма просмотра отчета ***VMware CI***
3.9	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**
3.10	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог его размещения и нажать кнопку ***Сохранить***	В указанном месте сохранен файл с указанным именем, в котором содержится отчет о результатах проверки целостности контролируемых на гипервизоре ***VMware ESXi*** файлах
3.11	В форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
3.12	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять текущую версию за эталон***	В форме сравнения отчетов пропала кнопка ***Принять текущую версию за эталон***
4	Просмотр результатов информирования администратора безопасности о результатах выполнения проверок контроля целостности программного обеспечения виртуальной инфраструктуры	
4.1	На рабочей станции ***Console*** запустить MS Outlook	Открытие окна MS Outlook
4.2	Просмотреть сообщения, полученные от пользователя, указанного в обработчике события нарушения целостности отчета	В сообщениях содержится информация о нарушениях целостности отчета
5	Просмотр списка событий в локальной консоли ПК	
5.1	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов, выполнении триггеров и сообщения о нарушении целостности загруженных отчетов

Критерии оценки:

Результаты проверки считаются положительными, если программный комплекс выполняет:

– контроль целостности компонентов, критически важных для функционирования хостовой операционной системы, гипервизора, гостевых операционных систем;

– контроль целостности состава и конфигурации виртуального оборудования;

– контроль целостности файлов, содержащих параметры настройки виртуализированного программного обеспечения и виртуальных машин;

– контроль целостности файлов-образов виртуализированного программного обеспечения и виртуальных машин, файлов-образов, используемых для обеспечения работы виртуальных файловых систем);

– контроль целостности резервных копий виртуальных машин (контейнеров);

– контроль состава аппаратной части компонентов виртуальной инфраструктуры.

1.6 Проверка регистрации событий безопасности

Описание функции:

Сервер ПК «Efros Config Inspector» v.3.1 обеспечивает регистрацию событий безопасности, которая заключается во внесении в используемую базу данных комплекса следующих событий:

– подключение (отключение) пользователей к серверу ПК;

– действия, выполняемые пользователями программного комплекса;

– операции, выполняемые на контролируемом оборудовании;

– события контроля программного обеспечения и конфигурации оборудования;

– сообщения, полученные с контролируемого оборудования.

Действия:

Проверка регистрации событий авторизации пользователей на сервере ПК выполняется на основании действий, выполненных в п. 1.2.1. В базе данных программного комплекса содержится информация о работе механизма идентификации и аутентификации пользователей на сервере ПК (дата и время, тип сообщения, описание сообщения, имя пользователя ПК, идентификатор пользователя ПК, идентификатор сессии).

Проверка регистрации сообщений о действиях пользователей ПК выполняется на основании действий, выполненных в п.п. 1.2.2, 1.2.3, 1.2.4. В базе данных программного комплекса содержится информация о действиях пользователей на сервере ПК (дата и время, имя устройства, тип сообщения, описание сообщения).

Проверка регистрации событий о выполняемых на контролируемом оборудовании операциях, контроле программного обеспечения и параметров конфигурации оборудования, регистрации полученных с контролируемого оборудования сообщений выполняется на основе действий, выполненных в п.п. 1.3.1, 1.4, 1.5.

Действия по настройке сроков хранения регистрируемых событий приведены в таблице 16.

Таблица 16 – Настройка сроков хранения регистрируемых событий

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи пользователя ПК **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК

№ п/п	Действия	Ожидаемый результат
3	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов, выполнении триггеров и сообщения о нарушении целостности загруженных отчетов
4	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Настройка***	В рабочей области консоли отобразился список параметров сервера ПК
5	В области *Администрирование* нажать кнопку ***База данных***	Открытие окна **«База данных»**.
6	В открывшемся окне отметить параметр ***Установить срок хранения событий*** и ввести в поле ввода значение ***2*** дня. Нажать кнопку ***Сохранить***	Успешное изменение срока хранения событий в базе данных, возврат во вкладку **Настройки**
7	Запустить серверную консоль и в области *Служба сервера* нажать кнопку ***Стоп***	Служба сервера ПК остановлена
8	В окне серверной консоли в области *Служба сервера* нажать кнопку ***Старт***	Служба сервера ПК запущена
9	На ЭВМ Console запустить клиентскую консоль и осуществить попытку подключения к серверу ПК от имени учетной записи **user1**	Открытие клиентской консоли ПК
10	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов, выполнении триггеров и сообщения о нарушении целостности загруженных отчетов за установленное в настройках время

Критерии оценки:

Результаты проверки считаются положительными, если на сервере ПК выполняется регистрация всех событий безопасности, связанных с работой пользователей на сервере ПК, в том числе регистрируется следующая информация:

– подключение (отключение) пользователей к серверу ПК;
– действия, выполняемые пользователями программного комплекса;
– операции, выполняемые на контролируемом оборудовании;
– события контроля программного обеспечения и конфигурации оборудования;
– сообщения, полученные с контролируемого оборудования.

1.7 Проверка управления конфигурациями контролируемого оборудования с сервера ПК

1.7.1 Проверка управления изменениями конфигурации сетевого оборудования

Описание функции:

Выполняется загрузка и проверка соответствия рабочей (running) и загрузочной (startup) конфигураций эталонам, установка эталонов, ведение истории версий отчетов с конфигурациями контролируемого оборудования, проверка и согласование рабочей и загрузочной конфигураций, восстановление загрузочной конфигурации, сравнение текстов конфигураций, экспорт текста отчета с конфигурацией оборудования в файл.

Действия:

Действия по проверке функций программного комплекса по управлению изменениями конфигураций сетевого оборудования приведены в таблице 17.

Таблица 17 – Управление изменениями конфигураций сетевого оборудования

№ п/п	Действия	Ожидаемый результат
1	Запустить клиентскую консоль ПК на ЭВМ ***CONSOL***	Открытие окна подключения консоли к серверу ПК
2	В окне подключения консоли к серверу ПК ввести логин и пароль учетной записи несуществующего на сервере ПК пользователя **user1** и нажать кнопку ***Подключиться***	Открытие клиентской консоли ПК
3	В панели выбора раздела клиентской консоли ПК нажать кнопку ***Устройства***	Отображается список контролируемых устройств, выполнение операций с которыми разрешено пользователю **user1**
4	В панели списка устройств выделить сетевое устройство ***Cisco IOS*** и в рабочей области перейти на вкладку **Отчеты**	Во вкладке **Отчеты** рабочей области отобразился список проверок и отчетов сетевого устройства ***Cisco IOS***
5	Проверить соответствие рабочей и загрузочной конфигурации устройства ***Cisco IOS***, для чего дважды щелкнуть левой кнопкой мыши по отчету ***Cisco IOS running-startup difference***	В рабочей области консоли открылась форма просмотра отчета ***Cisco IOS running-startup difference'*** – наличие несоответствий загрузочной и рабочей конфигураций устройства ***Cisco IOS***
6	Закрыть форму просмотра отчета ***Cisco IOS running-startup difference'***	Возврат во вкладку **Отчеты**
7	Дважды щелкнуть левой кнопкой мыши по отчету ***Cisco IOS 'show running'***	В рабочей области консоли открылась форма просмотра отчета ***Cisco IOS 'show running'***
8	В форме просмотра отчета нажать на кнопку ***Экспорт***	Открытие окна **«Сохранить как»**
9	В окне ввести имя файла, в котором будет сохранен отчет, указать каталог	В указанном месте сохранен файл с указанным именем, в котором содержится

№ п/п	Действия	Ожидаемый результат
	его размещения и нажать кнопку ***Сохранить***	отчет о конфигурации ***show running*** устройства ***Cisco IOS***
10	Сравнить последнюю загруженную версию отчета ***Cisco IOS 'show running'*** с эталоном, для чего в форме просмотра отчета нажать на ссылку ***Нарушение*** в поле *Статус*	Открытие формы сравнения текущего отчета с эталонным
11	В форме сравнения отчетов ознакомиться с результатами сравнения и нажать кнопку ***Принять текущую версию за эталон***	В форме сравнения отчетов пропала кнопка ***Принять текущую версию за эталон***
12	Последовательно закрыть формы сравнения и просмотра отчета	Возврат во вкладку **Отчеты** сетевого устройства ***Cisco IOS***
13	Перейти во вкладку **Статус** сетевого устройства ***Cisco IOS*** и нажать кнопку ***Скопировать running в startup*** в области *Действия с устройством*	Выполнение операции, в панели Последние действия отображаются сведения об успешном выполнении операции ***Скопировать running в startup***
14	Перейти во вкладку **Отчеты** сетевого устройства ***Cisco IOS***	Во вкладке **Отчеты** рабочей области отобразился список проверок и отчетов сетевого устройства ***Cisco IOS***
15	Проверить соответствие рабочей и загрузочной конфигурации устройства ***Cisco IOS***, для чего дважды щелкнуть левой кнопкой мыши по отчету ***Cisco IOS running-startup difference***	В рабочей области консоли открылась форма просмотра отчета ***Cisco IOS running-startup difference'*** – отсутствие несоответствий загрузочной и рабочей конфигураций устройства ***Cisco IOS***
16	В панели выбора раздела клиентской консоли ПК нажать кнопку **События**	Отображение сообщений аудита, фиксирующих события о загрузке отчетов, выполнении операций и сообщения о нарушении целостности контролируемых отчетов

Критерии оценки:

Проверка управления с сервера ПК конфигурациями сетевого оборудования считается успешной, если получены следующие результаты:

– при наличии отличий загруженных рабочей и загрузочной конфигурациях, в интерфейсе комплекса отображается информация об изменениях;

– выполнен экспорт содержимого отчета с конфигурацией оборудования в файл;

– операция согласования рабочей и загрузочной конфигураций прошла успешно.

1.7.2 Проверка регистрации данных об изменениях в конфигурации сетевого оборудования

Описание функции:

Сервер ПК «Efros Config Inspector» v.3.1 обеспечивает регистрацию данных об изменениях в конфигурации сетевого оборудования, которая заключается во внесении в используемую БД комплекса следующей информации:

– изменение конфигураций сетевого оборудования;

– хранение отчетов со всеми изменениями в конфигурации сетевого оборудования в течение установленного времени.

На сервере ПК реализована возможность сравнения загруженных версий отчетов о конфигурации сетевого оборудования.

Действия:

Проверка возможности сравнения загруженных версий отчетов и регистрации на сервере ПК данных об изменениях в конфигурации сетевого оборудования выполняется на основании действий, выполненных в п. 1.7.1. В базе данных программного комплекса содержатся все отчеты с данными об изменениях в конфигурации сетевого оборудования, за указанный в настройках комплекса срок хранения отчетов в архиве.

Критерии оценки:

Результаты проверки считаются положительными, если на сервере ПК:

– выполняется регистрация данных об изменениях в конфигурации сетевого оборудования;

– осуществляется сравнение загруженных версий отчетов о конфигурации сетевого оборудования;

– отчеты с данными конфигурации сетевого оборудования хранятся в базе данных комплекса в течение установленного времени.