МЕТОДИКА ФУНКЦИОНАЛЬНОГО ТЕСТИРОВАНИЯ РЕШЕНИЙ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

JET SECURITY TEAM

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
		Нефункциональные требования	
1	Автоматическое обновление базы уязвимостей по сети	1. Доступными средствами решения настроить автоматическое обновление базы уязвимостей по сети 2. Запустить обновление базы уязвимостей (при необходимости запуска вручную) 3. Убедиться, что база уязвимостей обновилась	Решение позволяет обновлять базу уязвимостей по сети в автоматическом режиме
2	Оффлайн-обновления базы уязвимостей	1. Произвести обновление базы уязвимостей в условиях отсутствия подключения компонентов (серверов) решения к Интернету 2. Убедиться, что база уязвимостей обновилась	Решение позволяет проводить офлайн-обновления базы уязвимостей
3	Открытый доступ к базе уязвимостей	1. Убедиться, что пользователь Системы имеет доступ к просмотру всех уязвимостей в базе через веб-интерфес решения	Пользователь Системы имеет доступ к просмотру всех уязвимостей в базе через веб-интерфес решения
4	Поддержка агентского сканирования	1. Произвести установку агента на тестовые на хосты (ОС Linux и ОС Windows, поддерживаемые решением) 2. Создать и запустить задачи сканирования с помощью агента для тестовых хостов 3. Убедиться, что задачи сканирования завершены успешно	Задачи агентского сканирования завершены успешно. По результатам сканирования в решении отображается найденная информация о конфигурации и уязвимостях тестовых хостов
5	Возможность работы с агентами без установки отдельного сервера	1. Установить агенты на тестовые хосты и настроить их взаимодействие с основной инсталляцией VM (без использования дополнительных серверов-посредников, прокси или коллекторов)	Решение не требует отдельного сервера для работы с агентами
6	Возможность обновления агентов встроенным механизмом продукта	1. Доступными средствами, встроенными по умолчанию в веб-интерфейс решения, запустить обновления агентов на ОС Windows и ОС Linux 2. Убедиться, что агенты на хостах успешно обновились	Решение позволяет обновлять агенты встроенными по умолчанию в веб-интерфейсе механизмами продукта
7	Поддержка распределенной установки модулей (компонентов) сканирования в разных сегментах сети	1. Установить дополнительный модуль (компонент) сканирования и подключить его к основной инсталляции 2. Убедиться, что сетевая связность актива с другими компонентами решения (кроме установленного модуля сканирования) отсутствует 3. Провести сканирование тестовых активов с помощью установленного модуля сканирования и убедиться, что сканирование завершено успешно	Решение поддерживает распределенную установку модулей (компонентов) сканирования для сканирования активов в частично изолированных сегментах сети
8	Поддержка мультиязычности	1. Убедиться, что в решении есть возможность выбора языка интерфейса во время установки или в веб-интерфейсе решения	Решение предоставляет возможность выбора языка, при этом в перечне поддерживаемых языков присутствует русский язык

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
9	Поддержка мультитенантности	1. В веб-интерфейсе решения создать дополнительный тестовый тенант / организацию. 2. Настроить принадлежность тестовых активов к созданному тенанту / организации 3. Войти в тестовый тенант / организацию. 4. Убедиться, что в тестовом тенанте отсутствуют хосты, задачи, УЗ и отчеты из любых других тенантов	Решение поддерживает сканирование геораспределенных филиалов и мультитенантность
10	Наличие сертификата соответствия ФСТЭК	На сайте ФСТЭК найти сертификат решения	Решение имеет действующий сертификат соответствия ФСТЭК
11	Присутствие решения в реестре отечественного ПО	Найти решение в реестре отечественного ПО	Решение присутствует в реестре отечественного ПО
	Мобильный сканер		
12	Наличие портативного (мобильного) сканера	1. Провести инсталляцию решения для использования в качестве мобильного сканера 2. Провести сканирование тестового актива 3. Изменить сетевые параметры устройства, на котором установлено решение 4. Провести сканирование тестового актива из другой подсети	Решение поддерживает установку на ноутбук для сканирования изолированных сегментов сети, без необходимости реконфигурации решения при переносе мобильного сканера в другие сегменты сети
13	Возможность переноса результатов сканирования мобильного сканера на основную инсталляцию	Проверка выполняется при успешном прохождении критерия №12 1. С помощью мобильного сканера провести сканирование тестовых активов из разных изолированных подсетей 2. Перенести результаты сканирования активов из разных подсетей на основную инсталляцию	Решение позволяет переносить результаты сканирования с мобильного сканера на основную инсталляцию
14	Наличие функционала выпуска отчетов в мобильном сканере	Проверка выполняется при успешном прохождении критерия №12 1. С помощью мобильного сканера провести сканирование тестовых активов из разных изолированных подсетей 2. Выпустить отчет по проведенным сканированиям	Мобильный сканер решения поддерживает выпуск отчетов
	Управление активами		
15	Построение интерактивной карты сети	1. Провести сканирование активного сетевого оборудования и серверов в режиме «аудит» (сканирование с аутентификацией) 2. В веб-интерфейсе решения убедиться, что интерактивная карта сети построена	Решение позволяет строить интерактивную карту сети
16	Экспорт карты сети	1. Произвести экспорт карты сети в графическом формате (например, PNG, JPG, PDF, SVG)	Решение позволяет выгружать карту сети из интерфейса решения
17	Создание динамических групп активов	1. Создать динамическую группу с любым критерием (например, версия или тип ОС) 2. Изменить критерий, убедиться, что состав группы изменился	Решение позволяет создавать динамические группы активов
18	Кастомизация карточки актива	1. Добавить пользовательское поле в карточку актива	Решение позволяет добавлять пользовательские поля в карточку актива
19	Скоринг активов: расчет уровня критичности	1. Задать уровень критичности актива любым встроенным механизмом решения	Решение позволяет задать уровень критичности актива

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
20	Дедупликация данных об активах	1. Произвести добавление тестового актива по IP-адресу 2. Произвести добавление тестового актива по fqdn 3. Произвести сканирование тестового актива в режиме аудит (сканирование с аутентификацией) 4. По результатам сканирования убедиться, что актив не имеет дублей	Решение производит дедупликацию активов
21	Создание пользовательских отметок (тегов) для активов	1. Создать и установить пользовательский тег для актива	Решение поддерживает создание и установку пользовательских отметок (тегов) для активов
22	Хранение истории изменения актива	1. Доступными средствами в решении убедиться, что в системе хранится информация о состоянии актива (уязвимости и конфигурация) в разные моменты времени	Решение хранит историю изменения активов
23	Функционал патч-менеджмента	1. Запустить установку патча (обновление ОС или стороннего прикладного ПО) из веб-интерфейса решения 2. По результатам установки патча убедиться в его успешной установке	Решение имеет функционал патч-менеджмента
24	Запуск административных действий / команд, выполняемых на активах	1. Запустить произвольную команду на активе через веб-интерфейс решения и увидеть результат ее выполнения (например, ipconfig, ip a, hostnamectl) 2. Запустить административное действие на активе встроенными в веб-интерфейс механизмами (например, выключить / перезагрузить хост, запустить / остановить / перезапустить службу)	Решение позволяет выполнять преднастроенные или произвольные автоматизированные действия по администрированию активов
	Настройка общих правил и логики системы		
25	Создание и управление задачами на устранение уязвимостей	1. Выбрать найденную уязвимость в карточке актива / отчете и инициировать создание задачи на ее устранение 2. Поочередно перевести задачу в доступные для нее статусы (например: «Новая», «В работе», «Закрыта») 3. Подтвердить возможность автоматического создания задач на устранение уязвимостей	Решение позволяет формировать и управлять задачами на устранение уязвимостей
26	Назначение ответственных для задачи на устранение уязвимостей	В веб-интерфейсе решения: 1. Выбрать уязвимость и создать задачу на ее устранение 2. В созданной задаче назначить ответственное лицо или группу лиц для ее выполнения	Решение позволяет назначать ответственных для задачи на устранение уязвимостей
27	Назначение SLA для устранения уязвимостей	1. Выполнить сканирование тестового актива 2. Выбрать уязвимость, обнаруженную на активе и встроенными в веб-интерфейс решения механизмами назначить срок для ее устранения 3. Убедиться, что решение позволяет отслеживать назначенный срок для устранения уязвимостей в автоматическом режиме встроенными средствами решения (например, меняет статус задачи / уязвимости)	Решение позволяет назначать и управлять SLA для устранения уязвимостей
28	Поддержка сквозного поиска, фильтрации, сортировки по активам и уязвимостям	1. Произвести поиск по доступным параметрам уязвимостей и активов 2. В результатах поиска произвести фильтрацию и сортировку по доступным параметрам	Решение имеет функционал сквозного поиска, фильтрации и сортировки по активам и уязвимостям
29	Автоматизация управления параметрами уязвимости (например, перерасчет критичности, срока, способа устранения)	1. Доступным в решении способом создать правило для автоматического изменения параметров уязвимости (например, перерасчет критичности, срока, способа устранения) по определенному правилу / условию 2. Убедиться в применении правила	Решение позволяет настроить правила автоматической смены параметров уязвимости

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
		Функционал визуализации и отчетности	
30	Визуализация данных в виде настраиваемых виджетов	1. В интерфейсе решения создать виджеты для дашборда	Решение имеет функционал построения виджетов
31	Визуализация данных в виде настраиваемых дашбордов	1. В интерфейсе решения создать новый дашборд и добавить на него несколько виджетов	Решение имеет функционал создания и организации дашбордов
32	Возможность создания пользовательских отчетов	1. Перейти в настройки формирования отчетов 2. Проверить возможность настройки состава данных (например, уязвимости, активы, статусы уязвимостей, конфигурации активов) 3. Сформировать пользовательские отчеты и убедиться, что выгрузка отчетов доступна в различных форматах (например, PDF, DOCX, XLSX и других) 4. Произвести выгрузку созданных отчетов в различных форматах 5. Убедиться, что отчеты выгрузились успешно и содержат ожидаемые данные	Решение имеет возможность создания пользовательских отчетов в различных форматах
33	Выпуск отчетов по расписанию	1. Настроить расписание выпуска отчета 2. Убедиться, что отчет выпустился по расписанию в заданное время	Решение позволяет выпускать отчеты по расписанию
34	Расширенная кастомизация интерфейса и объектов	В веб-интерфейсе решения: 1. Изменить произвольно выбранный объект веб-интерфейса (например, наименование пункта меню пользователя, отображение или последовательность элементов меню) 2. Создать новый объект решения (например, кастомный пункт меню пользователя) 3. Убедиться, что новые объекты и внесенные изменения отображаются в веб-интерфейсе	Решение поддерживает расширенную кастомизацию интерфейса и объектов
		Поддерживаемые типы активов для сканирования	
35	Поддержка сканирования ОС: Windows Server, Windows, Alma Linux, Ubuntu, Debian	1.Создать задачи на сканирование данных типов активов в режимах «пентест» (сканирование без аутентификации) и «аудит» (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита и пентеста для данных типов активов	Решение поддерживает сканирование в режимах «пентест» и «аудит» обозначенных типов активов
36	Поддержка сканирования отечественных ОС: AstraLinux, Alt Linux, РедОС	1.Создать задачи на сканирование данных типов активов в режимах «пентест» (сканирование без аутентификации) и «аудит» (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита и пентеста для данных типов активов	Решение поддерживает сканирование в режимах «пентест» и «аудит» обозначенных типов активов
37	Поддержка сканирования сетевого оборудования	1.Создать задачи на сканирование данных типов активов в режимах «пентест» (сканирование без аутентификации) и «аудит» (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать активы и обнаруживать уязвимости в режиме аудита и пентеста для данных типов активов	Решение поддерживает сканирование в режимах «пентест» и «аудит» обозначенных типов активов

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
38	Поддержка идентификации периферийных устройств (например, камеры, IP-телефония, принтеры)	1.Создать задачи на сканирование сети, в которой присутствуют периферийные устройства 2. Запустить задачу и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет идентифицировать периферийные устройства	Решение поддерживает идентификацию периферийных устройств
39	Поддержка сканирования СУБД (например, Oracle, PostgreSQL, MSSQL)	1. Создать задачи на сканирование СУБД в режиме «аудит» (сканирование с аутентификацией) с использованием УЗ для подключения к СУБД 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет получить информацию о конфигурации СУБД	Решение поддерживает сканирование обозначенных типов активов
40	Поддержка сканирования серверного ПО (например, веб-серверы, службы каталогов, почтовые сервера, системы виртуализации)	1. Создать задачи на сканирование активов, имеющих серверное ПО, в режиме «аудит» (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет обнаруживать уязвимости в режиме аудита для серверного ПО	Решение поддерживает сканирование серверного ПО
41	Инвентаризация и поиск уязвимостей в контейнерах	1. Создать задачи на сканирование активов, использующих контейнеризацию, в режиме «аудит» (сканирование с аутентификацией) 2. Запустить задачи и убедиться в их успешном выполнении 3. Ознакомиться с результатами сканирования и убедиться, что решение позволяет получить инвентаризационные данные и обнаруживать уязвимости в режиме аудита для активов с контейнеризацией	Решение позволяет получить информацию о контейнерах и найденных в них уязвимостей
	Возможности интеграции		
42	Наличие документированного API	1. В документации производителя найти информацию об использовании API 2. Получить список активов средствами API	Решение предоставляет документированное API
43	Разграничение доступа для API-ключей	1. При создании API-ключа убедиться в возможности разграничения доступа	Решение позволяет разграничивать доступ для API-ключей
44	Наличие собственных / встроенных средств мониторинга работоспособности (Health-Check)	1. В веб-интерфейсе решения перейти на страницу / раздел с мониторингом работоспособности решения (HealthCheck) 2. Убедиться, что отображаются метрики работоспособности решения (например, статус служб, загрузка CPU/RAM, доступность компонентов решения, состояние базы уязвимостей, сетевые подключения)	Решение предоставляет встроенный функционал мониторинга работоспособности
45	Возможность интеграции с системами мониторинга работоспособности	1. Убедиться, что в решении доступна встроенная поддержка интеграции с системами мониторинга с готовыми механизмами передачи метрик работоспособности (например, статус служб, загрузка CPU/RAM, состояние компонентов и подобного) без необходимости разработки скриптов.	Решение предоставляет стандартные интерфейсы для интеграции с системами мониторинга без необходимости разработки скриптов
46	Поддержка доменной аутентификации и авторизации	1. Настроить подключение к службе каталогов 2. Проверить возможность аутентификации и авторизации под доменной УЗ	Решение поддерживает доменную аутентификацию и авторизацию
47	Интеграция с Service Desk/ITSM-системами	1.Убедиться, что в решении доступна встроенная поддержка интеграции с Service Desk/ITSM-системами (например, Jira, ServiceNow, BMC Remedy, Freshservice) с готовыми механизмами передачи данных без необходимости разработки скриптов	Решение предоставляет стандартные интерфейсы для интеграции с Service Desk/ITSM системами без необходимости разработки скриптов

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
48	Интеграция с SIEM в части отправки событий системы VM	1.Убедиться, что доступна встроенная поддержка отправки событий системы управления уязвимостями (например, аутентификация и авторизация пользователей в веб-интерфейсе) во внешние SIEM-системы (например, MP SIEM, KUMA, Splunk, QRadar) через готовые коннекторы	Решение поддерживает интеграцию с SIEM в части отправки событий системы
49	Функционал получения данных об активах из смежных систем (например, из службы каталогов, среды виртуализации, SIEM-системы, смежных сканеров)	1. Выполнить импорт активов из смежной системы 2. Убедиться в корректном отображении и актуальности полученных данных	Решение имеет функционал получения данных об активах из смежных систем
50	Отправка оповещений о событиях в системе (например, появления нового актива, важной уязвимости на активе, обновление базы уязвимостей)	1. Настроить и проверить наличие встроенной возможности отправки почтовых уведомлений о системных событиях (например, обнаружение нового актива, выявление уязвимости с заданным уровнем критичности, обновление базы уязвимостей)	Решение поддерживает настройку и автоматическую отправку оповещений о событиях в системе
	Управление сканированием и уязвимостями		
51	Кастомизация карточки уязвимости	1. Доступными механизмами веб-интерфейса решения выполнить преобразования карточки уязвимости: дополнить / добавить блок ссылок на внешние источники пользовательскими ссылками, дополнить описание уязвимости, создать дополнительный информационный блок в карточке уязвимости 2. В веб-интерфейсе решения перейти в карточку уязвимости и убедиться, что внесенные изменения успешно применены	Решение позволяет кастомизировать карточку уязвимости
52	Создание пользовательских отметок (тегов) для уязвимостей	1. Создать и установить пользовательский тег для актива	Решение позволяет создавать пользовательские метки (теги) для уязвимостей
53	Расписание сканирований	1. Настроить запуск задания (задачи) на сканирование по расписанию 2. Убедиться в запуске задачи в указанное время	Решение позволяет проводить сканирования по расписанию
54	Поиск уязвимостей без повторного сканирования хостов (ретро-скан)	1. Убедиться, что решение выявляет новые уязвимости без необходимости проведения повторного сканирования актива	Решение позволяет находить уязвимости без необходимости проведения повторного сканирования
55	Возможность исключить актив из сканирования в заданные временные интервалы	1.В веб-интерфейсе решения перейти в раздел управления активами 2. Для тестового актива задать временной интервал (например, дата и время начала / окончания), в течение которого сканирование не должно выполняться 3. В запрещенный интервал времени для актива запустить сканирование и убедиться, что оно не выполняется	Решение позволяет настроить исключение актива из сканирования в заданный период, и в указанный интервал сканирование этого актива не запускается автоматически, даже если он входит в состав регулярных заданий
56	Брутфорс с использованием пользовательских справочников	1. Загрузить или указать пользовательский справочник (список логинов и / или паролей) и назначить его для использования при брутфорс-атаке на целевой сервис 2. Запустить сканирование тестового хоста и убедиться, что в результатах сканирования есть подобранные учетные данные	Решение поддерживает использование внешних (пользовательских) словарей при проведении брутфорс-проверок и применяет их при сканировании целевых сервисов
57	Настройка правил и логики политик / профилей сканирования	1. Доступными средствами настроить правила сканировании в задаче (например, список портов, протоколов, методов авторизации) 2. Запустить задачу и убедиться в успешном ее завершении с учетом заданных правил	Решение позволяет настраивать правила и логику политик / профилей сканирования

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
58	Возможность использования нескольких УЗ разного типа в одной задаче с автоматическим подбором.	1.Создать задачу сканирования в режиме «аудит» (сканирование с аутентификацией) для тестовых хостов (Windows и Linux) 2. В параметрах подключения указать две учетные записи разного типа (УЗ Windows, УЗ SSH) 3. Убедиться, что сканирование на обоих хостах завершилось успешно	Решение автоматически выбирает и применяет подходящую учетную запись для каждого типа активов в рамках одной задачи сканирования
59	Проверка доступности хоста до сканирования	1. Доступным в решении способом запустить проверку доступности хоста без запуска сканирования 2. Убедиться в выводе результата проверки доступности	Решение позволяет проверять доступность хоста до сканирования
60	Проверка учетных записей до сканирования	1. Доступным в решении способом запустить проверку учетной записи для сканирования в режиме белого ящика без запуска сканирования 2. Убедиться в выводе результата проверки доступности	Решение позволяет проверять корректность учетной записи до сканирования
61	Клонирование задачи сканирования	1. Создать задачу на сканирование в режиме «аудит» и указать необходимые настройки сканирования (цель сканирования, профиль / политику сканирования, УЗ для подключения к активу) 2. Скопировать / склонировать созданную задачу 3. Убедиться, что в копии задачи присутствуют все ранее выполненные настройки	Решение позволяет клонировать задачи сканирования
62	Клонирование профиля / политики сканирования	1. Создать профиль / политику на сканирование в режиме «пентест» и указать необходимые настройки сканирования (перечень портов, протоколов, проверок) 2. Скопировать / склонировать созданный профиль / политику 3. Убедиться, что в копии профиля / политики присутствуют все ранее выполненные настройки	Решение позволяет клонировать профили / политики сканирования
63	Отображение прогресса сканирования в реальном времени	1. В веб-интерфейсе решения убедиться, что для запущенной задачи сканирования отображается прогресс сканирования в виде количества обработанных хостов из общего числа	Решение отображает прогресс сканирования в реальном времени
64	Пауза задачи сканирования	1. Поставить на паузу запущенную задачу на сканирование и убедиться в ее остановке 2. Подождать 5 минут 3. Снять с паузы задачу и убедиться в продолжении ее выполнения 4. Убедиться, что задача завершилась успешно	Решение позволяет ставить задачи сканирования на паузу
65	Добавление исключений для уязвимостей и ПО	1. Провести сканирование актива в режиме «аудит» (сканирование с аутентификацией) 2. Добавить в исключение одну из найденных уязвимостей 3. Провести повторное сканирование и убедиться в отсутствии исключенной уязвимости	Решение позволяет добавлять исключения для уязвимостей и ПО
66	Ведение и отображение идентификаторов уязвимостей (CVE, NVD, БДУ, CWE)	1. В результатах ранее проведенного сканирования найти информацию о CVE, CPE, CWE и БДУ для уязвимостей	Решение предоставляет информацию о CVE, CPE, CWE и БДУ для уязвимостей
67	Поддержка CVSS версии 2	1. Убедиться, что в данных об обнаруженных уязвимостях есть оценка критичности по CVSS версии 2	Решение предоставляет информацию об обнаруженных уязвимостях с указанием оценки критичности по CVSS версии 2
68	Поддержка CVSS версии 3	1. Убедиться, что в данных об обнаруженных уязвимостях есть оценка критичности по CVSS разных версий 3	Решение предоставляет информацию об обнаруженных уязвимостях с указанием оценки критичности по CVSS версии 3

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
69	Поддержка CVSS версии 4	1. Убедиться, что в данных об обнаруженных уязвимостях есть оценка критичности по CVSS разных версии 4	Решение предоставляет информацию об обнаруженных уязвимостях с указанием оценки критичности по CVSS версии 4
70	Добавление собственной проверки уязвимостей	1. Создать собственную проверку на уязвимости 2. Запустить сканирование с данной проверкой и убедиться в корректности работы	Решение позволяет добавлять собственные проверки уязвимостей
71	Настраиваемый скоринг уязвимостей	1. В веб-интерфейсе решения изменить критичность уязвимости	Решение позволяет настраивать критичность уязвимости
72	Встроенный расчет вероятности того, что уязвимость будет использована в реальных атаках для уязвимостей	1. В результатах ранее проведенного сканирования найти информацию о вероятности того, что уязвимость будет использована в реальных атаках для уязвимостей	Решение производит расчет вероятности использования в реальных атаках для уязвимостей
73	Отображение информации о наличии эксплойта для уязвимости	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Проверить наличие поля или индикатора, явно указывающего на наличие публичного эксплойта	В решении отображается информация о наличии публичного эксплойта
74	Путь установки уязвимой сущности	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Убедиться в наличии информации о пути установки уязвимой сущности	Решение предоставляет информацию о пути установки уязвимых сущностей
75	Ссылки на внешние сервисы в карточке уязвимости (NVD, Exploit-DB, БДУ ФСТЭК и другие)	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Проверить наличие гиперссылок на внешние справочные ресурсы: NVD, Vulners.com, Exploit-DB, Базу данных уязвимостей ФСТЭК России (БДУ)	В карточке уязвимости присутствуют ссылки на соответствующие страницы внешних сервисов (NVD, Vulners.com, Exploit-DB, БДУ ФСТЭК), позволяющие быстро перейти к дополнительной информации.
76	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Проверить наличие рекомендаций по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК или ссылки на источник	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК
77	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Проверить наличие рекомендаций по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ или ссылки на источник	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ
78	Расчет критичности уязвимости по методике ФСТЭК	1. Убедиться в наличии расчета критичности уровня уязвимости по методике ФСТЭК	Решение позволяет рассчитывать критичность уязвимости по методике ФСТЭК
79	Проверка обновлений по БДУ ФСТЭК	1. Убедиться, что в веб-интерфейсе решения предлагаемые к установке обновления (Linux, Windows) протестированы ФСТЭК	Решение позволяет проверять обновления по БДУ ФСТЭК
80	Отображение информации о трендовости уязвимости	1. В веб-интерфейсе решения открыть карточку уязвимости / результаты сканирования 2. Проверить наличие индикатора или поля, отражающего трендовость уязвимости (например, «актуальная», «в фокусе злоумышленников», «часто эксплуатируемая», «входит в Top N уязвимостей», «трендовая»)	Решение отображает информацию о трендовости уязвимостей
	Оценка соответствия		
81	Проверка активов на соответствие предустановленным стандартам защищенной конфигурации	1. Запустить задачу на проверку соответствия стандартам для тестового хоста с несоответствиями требованиям. 2. После выполнения задачи убедиться, что для хоста указаны соответствия и несоответствия требованиям.	Решение позволяет проводить проверку на соответствие стандартам защищенной конфигурации

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
82	Наличие конструктора для создания пользовательских требований конфигураций	1. В веб-интерфейсе решения создать пользовательское требование проверки конфигурации 2. Запустить задачу на проверку соответствия пользовательского требования 3. Убедиться, что проверка требования выполнена успешно	Решение позволяет создавать пользовательские требования конфигураций во встроенном конструкторе
83	Наличие рекомендаций по исправлению несоответствий конфигураций	1. Выбрать тестовые хосты (Linux, Windows) с некорректными настройками стандартов защищенной конфигурации и запустить задачи на проверку соответствия 2. После выполнения задачи убедиться, что для тестовых хостов указаны несоответствия требованиям и даны рекомендации по приведению настроек к требуемым значениям	Решение предоставляет рекомендации по исправлению несоответствий конфигураций
84	Ведение истории оценки соответствия	1. Выбрать тестовые хосты (Linux, Windows) с некорректными настройками стандартов защищенной конфигурации и запустить задачи на проверку соответствия 2. На тестовых хостах привести один из параметров к требуемому значению 3. Повторно запустить задачу на проверку соответствия стандартам 4. Убедиться в возможности просмотра результатов обоих сканирований	Решение хранит историю оценки соответствия
85	Встроенные механизмы сравнения результатов оценки соответствия	1. Выбрать тестовые хосты (Linux, Windows) с отсутствующими или некорректными настройками стандартов защищенной конфигурации и запустить задачи на проверку соответствия 2. На тестовых хостах привести один из параметров к требуемому значению 3. Повторно запустить задачу на проверку соответствия стандартам 4. Встроенными в веб-интерфейс механизмами сравнить результаты сканирования (например, выпустить дифференциальный отчет, проверить изменение статуса для исправленного параметра, запустить задачу на сравнение результатов и убедиться, что однозначно возможно определить изменения)	Решение имеет встроенные механизмы сравнения результатов оценки соответствия
	Сканирование веб-ресурсов		
86	Возможность аутентификации в веб-приложении (cookie, логин-пароль, заголовки и их значения)	1. Настроить задачу на сканирование тестовых веб-ресурсов с использованием аутентификации 2. Провести сканирование и убедиться, что сканирование с аутентификацией прошло успешно	Решение поддерживает сканирование с аутентификацией для веб-ресурсов
87	Сканирование в режиме поиска поддоменов	1. Настроить задачу на сканирование тестовых веб-ресурсов для поиска поддоменов 2. Провести сканирование и убедиться, что в результатах сканирования присутствует информация о найденных поддоменах	Решение имеет функционал поиска поддоменов
88	Поиск скрытых файлов и папок на сервере	1. Настроить и запустить задачу на сканирование сайта для поиска скрытых файлов и папок 2. Провести сканирование и убедиться, что в результатах сканирования присутствует информация о найденных скрытых файлах / папках	Решение имеет функционал поиска скрытых файлов и папок
89	Сканирование в режиме имитации атаки	1. Провести сканирование веб-ресурса в режиме имитации атаки 2. Убедиться, что в результатах доступна информация о параметрах проведения имитации атаки (например, ответ веб-сервера, используемые SQL-инъекции и прочее).	Решение имеет функционал сканирования ресурсов в режиме атаки
90	Обнаружение уязвимостей категории Injection (SQL-инъекции, загрузка файлов, Code-инъекции)	1. Провести сканирование уязвимых веб-ресурсов 2. В результатах сканирования найти уязвимости типа «Code & Command Injection» Например, Server Side Code Injection, Remote OS Command Injection, SQL Injection, LDAP Injection, Command Injection, XPath Injection, Server Side Include, Insecure Deserialization	Решение обнаруживает уязвимости типа «Code & Command Injection»

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
91	Обнаружение уязвимостей аутентификации, авторизации и сессии (CSRF) в веб-ресурсах	1. Провести сканирование уязвимых веб-ресурсов 2. В результатах сканирования найти уязвимостей типа «Cross-Site Request Forgery»	Решение обнаруживает уязвимости типа «Cross-Site Request Forgery»
92	Обнаружение клиентских и браузерных уязвимостей (Client-Side Attacks, cookie issues, security headers, memory safety issues)	1. Провести сканирование уязвимых веб-ресурсов 2. В результатах сканирования найти уязвимости, связанные с обработкой данных на стороне браузера пользователя Например, XSS (Cross-Site Scripting), Script ActiveX Object, Cookie No HttpOnly Flag, Cookie No Secure Flag, Buffer Overflow, Format String, Integer Overflow, X-Permitted Cross-Domain-Policies Header Missing, X-XSS-Protection Header Missing, Strict-TransportSecurity Header Missing	Решение обнаруживает клиентские и браузерные уязвимости
93	Обнаружение уязвимостей типа «Cryptographic Weaknesses»	1. Провести сканирование уязвимых веб-ресурсов 2. В результатах сканирования найти уязвимости типа «Cryptographic Weaknesses» Например, Weak Cipher Suite, Heartbleed (OpenSSL)	Решение обнаруживает уязвимости типа «Cryptographic Weaknesses»
94	Обнаружение уязвимостей типа «Information Disclosure»	1. Провести сканирование уязвимых веб-ресурсов 2. В результатах сканирования найти уязвимости типа «Information Disclosure» Например, PII Disclosure, Information Disclosure, Private IP Disclosure, Sensitive Information in HTTP Headers, Insecure Content	Решение обнаруживает уязвимости типа «Information Disclosure»
	Безопасность		
95	Наличие настраиваемой ролевой модели	В веб-интерфейсе решения: 1. Создать новую пользовательскую роль 2. Для роли настроить доступ к произвольно выбранным разделам веб-интерфейса или другим объектам решения (например, группа активов) 3. Назначить тестовому пользователю созданную роль 4. Авторизоваться под УЗ тестового пользователя и убедиться, что доступ пользователя соответствует настроенной роли	Решение позволяет настраивать ролевую модель и ограничивать права доступа к объектам решения
96	Возможность настройки парольной политики - настраиваемая сложность пароля (буквы, цифры, заглавные, спецсимволы) - история ранее заданных паролей - минимальная длина паролей - время жизни пароля	В веб-интерфейсе решения: 1. Настроить парольную политику (буквы, цифры, спецсимволы, история на 5 паролей, минимальная длина 10 символов, время жизни пароля — 24 часа) 2. Для тестового пользователя задать пароль, несоответствующий требованиям сложности, и убедиться, что решение не позволяет этого сделать 3. Для тестового пользователя 2 раза сменить пароль, при этом первый и третий пароли должны быть одинаковыми, и убедиться, что решение не позволяет этого сделать 4. Для тестового пользователя задать пароль меньше минимальной длины и убедиться, что решение не позволяет этого сделать 5. Для тестового пользователя задать пароль соответствующий требованиям. Через 24 часа авторизоваться с тестовой УЗ и убедиться, что решение не позволяет этого сделать	Решение позволяет гибко настраивать парольную политику
97	Механизмы блокировки учетных записей после нескольких неудачных попыток входа	1. При авторизации в веб-интрефейсе решения ввести 8 раз неправильный пароль для тестовой УЗ 2. При авторизации в веб-интрефейсе решения ввести правильный пароль для тестовой УЗ 3. Любыми доступными в решении средствами убедиться, что УЗ заблокирована	Решение имеет функционал блокировки учетных записей
98	Шифрование критичных данных (в том числе с использованием пользовательских ключей шифрования)	1. При установке решения или в веб-интерфейсе решения указать пользовательский ключ шифрования 2. Убедиться, что в базе данных решения пароли хранятся в зашифрованном виде	Решение хранит критичные данные в зашифрованом виде, в том числе с использованием пользовательских ключей шифрования

№	КРИТЕРИЙ	ШАГИ	ОЖИДАЕМЫЙ РЕЗУЛЬТАТ
99	Создание и восстановление из резервной копии системы	1. Методами, входящими в комплект поставки решения, выполнить резервное копирование 2. В веб-интерфейсе решения удалить любой актив и задачу 3. Восстановить систему из резервной копии 4. Убедиться, что удаленный актив и задача восстановлены	Решение имеет функционал резервного копирования и восстановления
	Производительность и эффективность		
100	Скорость добавления новых уязвимостей в базу уязвимостей решения: время между появлением новой уязвимости в публичных базах (например, NVD, БДУ ФСТЭК) и ее добавлением в сканер	1. На сайте nvd.nist.gov выбрать новые уязвимости для поддерживаемого ПО / ОС. 2. Проконтролировать, через какое время выбранные уязвимости появятся в базе уязвимостей решения.	Время появления новых уязвимостей в базе уязвимостей решения зафиксировано
101	Настройка интенсивности (скорости) сканирования в веб-интерфейсе	Для сканирования в режиме «аудит» (сканирование с аутентификацией): 1. В веб-интерфейсе решения настроить интенсивность сканирования в 1 поток 2. В рамках одной задачи просканировать 3 хоста 3. В веб-интерфейсе решения настроить интенсивность сканирования в 4 потока 4. В рамках одной задачи просканировать 3 хоста 5. Доступными в решении средствами (например, время выполнения задачи, история или логи задачи) убедиться в возможности настройки и корректности работы интенсивности сканирования	Решение имеет функционал настройки интенсивности сканирования для задач сканирования в режиме «аудит» (сканирование с аутентификацией)
102	Возможность выбора нескольких модулей (компонентов) сканирования на одну задачу	1. В веб-интерфейсе решения создать задачу на сканирование нескольких хостов. 2. В параметрах задачи указать 1 модуль (компонент) сканирования и запустить задачу 3. Зафиксировать время выполнения задачи 4. В параметрах задачи указать несколько модулей (компонентов) сканирования и запустить задачу 5. Зафиксировать время выполнения задачи 6. Доступными в решении средствами убедиться, что сканирование происходит одновременно несколькими модулями (компонентами) сканирования в рамках одной задачи. При этом общее время сканирования активов уменьшается	Решение поддерживает сканирование несколькими модулями (компонентами) сканирования в рамках одной задачи