ТЕСТИРОВАНИЕ РЕШЕНИЙ ПО УПРАВЛЕНИЮ УЯЗВИМОСТЯМИ

JET SECURITY TEAM

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Общая организационная информация	
1.1	Автоматическое обновление базы уязвимостей по сети	1. Запустить автоматическое обновление базы уязвимостей через интерфейс управления сканером. 2. Проверить версию баз данных.	Решение позволяет обновлять базу уязвимостей по сети в автоматическом режиме.
1.2	Возможность офлайн-обновления базы уязвимостей сканера	1. На выделенном (изолированном) сканере обновить базу уязвимостей без подключения к интернету. 2. Проверить версию базы уязвимостей этого сканера.	Решение позволяет проводить офлайн-обновления базы уязвимостей.
1.3	Централизованное управление через веб-интерфейс	1. Убедиться в доступности веб-интерфейса для управления решением. 2. Проверить возможность управления всеми компонентами системы через веб-интерфейс.	Решение предоставляет возможность управления всеми компонентами системы через веб-интерфейс.
1.4	Возможность установки агентов на хосты	1. В соответствии с документацией произвести установку агента на хосты (Linux, Windows).	Решение позволяет устанавливать агенты на хосты.
1.5	Возможность работы в частично или полностью изолированных сегментах сети	1. На выделенном (изолированном) сканере обновить базу уязвимостей без подключения к интернету. 2. Проверить версию базы уязвимостей этого сканера. 3. Произвести сканирование изолированного сегмента с конфигурацией для изолированного сегмента.	Решение позволяет производить сканирование изолированного сегмента с обновленной базой уязвимостей.
1.6	Локализация интерфейса и поддержка мультиязычности	1.Открыть интерфейс управления решением. 2. Настроить язык интерфейса. 3. Определить список поддерживаемых языков.	Решение предоставляет возможность смены локализации интерфейса, при этом в перечне поддерживаемых языковых локализаций присутствует русский язык.
1.7	Наличие сертификата ФСТЭК и присутствие решения в реестре отечественного ПО	1. На сайте ФСТЭК найти сертификат решения. 2. Найти решение в реестре отечественного ПО.	1. Решение имеет действующий сертификат ФСТЭК. 2. Решение присутствует в реестре отечественного ПО.
		Управление активами	
2.1	Построение интерактивной карты сети	1. По результатам сканирований произвести построение карты сети.	Решение позволяет формировать интерактивную карту сети.
2.2	Создание динамических групп активов	1. Создать группу активов, где активы перечислены списком. 2. Создать группу активов, где активы объединены по типу ОС. 3. Зафиксировать состав созданных групп. 4. Произвести настройку задачи с ранее не использованными целями. 5. Убедиться, что группа активов, созданная в пункте второй проверки, изменила свой состав.	Решение позволяет создавать динамические группы активов.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Управление активами	
2.3	Поиск по группам активов	1. В интерфейсе решения произвести поиск по имени группы. 2. В интерфейсе решения произвести поиск актива в определенной группе.	Решение позволяет производить поиск по группам активов.
2.4	Кастомизация карточки актива и уязвимости	1. Убедиться в возможности добавления кастомных полей в карточку актива.	Решение позволяет добавлять кастомные поля в карточки актива.
2.5	Скоринг активов: расчет уровня критичности	1. В результатах сканирования определить оценку критичности для актива.	Решение выполняет скоринг активов в части расчета уровня критичности.
2.6	Дедупликация данных об активах	1. Убедиться, что в результатах сканирований нет дубликатов активов.	Решение не создает и не хранит дубликаты активов.
2.7	Тегирование активов	1. Для активов с Active Directory установить соответствующий тег.	Решение поддерживает установку пользовательских отметок (тегов) для активов.
		Настройка общих правил и логики системы	
3.1	Импорт и экспорт политик и результатов сканирования между инсталляциями в рамках одного решения	1. Произвести импорт и экспорт политик и результатов сканирования в доступном формате. 2. Убедиться, что эти данные доступны для обмена между инсталляциями.	Решение позволяет импортировать данные.
3.2	Встроенный функционал ведения процесса устранения уязвимости	1. По результатам сканирования сформировать задачу на устранения уязвимостей, назначить ответственных. 2. Проверить отображение истории работы по устранению уязвимости.	Решение имеет встроенный функционал ведения процесса устранения уязвимости.
3.3	Настройка правил отправки оповещений	1. Для ранее созданного расписания настроить отправку уведомлений о завершении сканирования.	Решение позволяет отправлять уведомление о завершении сканирования.
3.4	Поддержка сквозного поиска, фильтрации, сортировки по активам и уязвимостям	1. Произвести поиск по названию уязвимости. 2. В результатах поиска произвести фильтрацию типу ОС и сортировку по дате в обратном порядке.	Решение имеет функционал сквозного поиска, фильтрации и сортировки по активам и уязвимостям.
3.5	Функционал патч-менеджмента	1. Открыть карточку объекта и выбрать уязвимость, для которой возможно устранение посредством установки патча. 2. Запустить установку патча безопасности из интерфейса решения. 3. По результатам установки патча провести повторное сканирование и убедиться в устранении уязвимости.	Решение имеет функционал патч-менеджмента.
3.6	Настройка правил автоматической смены статуса уязвимости (перерасчета критичности, срока, способа устранения)	1. В результатах ранее проведенного сканирования произвести настройку ложного срабатывания для одной из обнаруженных уязвимостей. 2. Произвести принятие риска для одной из обнаруженных уязвимостей. 3. Оценить влияние на итоговую оценку защищенности актива.	Решение позволяет настроить правила автоматической смены статуса уязвимости.
3.7	Визуализация данных в виде настраиваемых виджетов и дашбордов	1. В интерфейсе решения настроить отображение дашбордов.	Решение имеет функционал построения виджетов и организации дашбордов.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Поддерживаемые типы активов для сканирования	
4.1	Поддержка сканирования ОС	1.Создать задачи на сканирование данных типов активов в режиме 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 обозначенных типов активов.
4.2	Поддержка сканирования сетевого оборудования	1.Создать задачи на сканирование данных типов активов в режиме 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 обозначенных типов активов.
4.3	Поддержка сканирования периферийного оборудования	1.Создать задачи на сканирование данных типов активов в режиме 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 обозначенных типов активов.
4.4	Поддержка сканирования ИТ-решений	1.Создать задачи на сканирование данных типов активов в режиме 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 обозначенных типов активов.
4.5	Поддержка сканирования ИБ-решений	1.Создать задачи на сканирование данных типов активов в режиме 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 обозначенных типов активов.
4.6	Инвентаризация и поиск уязвимостей в запущенных контейнерах	1. Настроить задачу для сканирования запущенных контейнеров. 2. Получить результаты сканирования с найденными уязвимостями в запущенных контейнерах.	Решение позволяет получить информацию о запущенных контейнерах и найденных в них уязвимостях.
		Возможности интеграции	
5.1	Наличие документированного API для: a. Получения результатов сканирования (получения активов и уязвимостей) b. Заведение профилей/задач сканирования c. Запуска сканирования	1. В документации производителя найти информацию об использовании API. 2. Средствами API получить результаты ранее завершенного сканирования. 3. Создать новую задачу средствами API. 4. Запустить созданную задачу средствами API.	В документации есть подробное описание API (Endpoint, авторизация, примеры использования). API позволяет создавать и запускать задачи, получать результаты сканирований.
5.2	Возможность интеграции с системами мониторинга работоспособности	1. Настроить отправку метрик в систему мониторинга работоспособности. 2. Настроить мониторинг решения средствами системы мониторинга работоспособности.	В системе мониторинга работоспособности присутствуют данные из сканера.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Возможности интеграции	
5.3	Интеграция с Micorosoft Active Directory	1. Настроить подключение к службе каталогов и получить данные с контроллера домена. 2. Провести синхронизацию и настроить авторизацию для доменных пользователей в интерфейсе решения. 3. Создать задачу сканирования списка целей из Active Directory. 4. Настроить режим сканирования без авторизации.	Решение позволяет выполнять сканирование ресурсов, авторизацию в решении с использованием доменных УЗ, взятых из Active Directory.
5.4	Интеграция с SIEM	1. Проверить наличие возможности интеграции SIEM в официальной документации вендора.	Решение предполагает интеграцию с SIEM.
		Управление сканированием и уязвимостями	
6.1	Расписание сканирований	1. Настроить последовательный запуск ранее созданных задач по расписанию с интервалом старта в несколько минут между каждой задачей. 2. Поверить, что задачи запустились в назначенное время. 3. После завершения выполнения задач зафиксировать суммарное время сканирования. (Эти данные будут использоваться в проверке: Обработка больших объемов данных: Производительность при работе с инфраструктурой, содержащей сотни тысяч активов.)	Решение позволяет проводить сканирования по расписанию.
6.2	Сканирование в режиме brute force для возможности перебора паролей в целевых системах	1. Создать задачу для подбора пароля к RDP и SSH по словарю.	Решение позволяет производить подбор паролей.
6.3	Настройка правил и логики профилей сканирования	1. Создать новый профиль сканирования. 2. Изменить настройки правил и логики нового профиля.	Решение позволяет производить настройку правил и логики профилей сканирования.
6.4	Настройка сканирования (выбор диапазонов подсетей/IP-адресов/портов)	1. Создать задачу сканирования с указанием подсетей/IP-адресов/портов.	Решение позволяет сканировать указанные подсети/IP-адреса/порты.
6.5	Прогнозирование рисков: Возможность оценки потенциального ущерба от эксплуатации уязвимостей	1. В результатах ранее проведенного сканирования найти соответствующую информацию.	Решение имеет функционал по прогнозированию рисков при возможной эксплуатации уязвимости.
6.6	Ведение и отображение идентификаторов уязвимостей (CVE, NVD, БДУ, CPE, CWE).	1. Убедиться, что в результатах присутствует информация о CVE, CPE, CWE и БДУ для уязвимостей.	Решение предоставляет информацию о CVE, CPE, CWE и БДУ для уязвимостей.
6.7	Поддержка CVSS-метрик версий 2/3/4 и возможности задания кастомных метрик CVSS	1. Убедиться, что в данных об обнаруженных уязвимостях есть оценка критичности по CVSS разных версий.	Решение предоставляет информацию об обнаруженных уязвимостях с указанием оценки критичности по CVSS разных версий.
6.8	Поддержка нотации OVAL, возможность добавления собственной проверки уязвимостей	1. Для уязвимости, обнаруженной в рамках сканирований, произвести просмотр ее параметров в нотации OVAL. 2. Создать новую проверку, описанную с помощью OVAL.	Решение поддерживает OVAL, позволяет добавить собственную проверку.
6.9	Настраиваемый скоринг уязвимостей	1. В результатах сканирования изменить критичность уязвимости.	Решение позволяет настраивать критичность уязвимости.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
Управление сканированием и уязвимостями			
6.10	Проверка эксплуатируемости уязвимости	1. Убедиться, что уязвимость отмечается в ПО как имеющая эксплойт.	Решение позволяет проверить эксплуатируемость уязвимости.
6.11	Дедупликация данных об уязвимостях	1. Найти в результатах сканирования актива уязвимости с дублями (например, дубликаты уязвимостей для разных сервисов). 2. Убедиться, что для дубликатов в карточках уязвимостей есть уникальные поля, позволяющие однозначно идентифицировать ее: что уязвимости не являются полной копией друг друга.	Решение позволяет дедуплицировать данные об уязвимостях.
6.12	Ссылки на внешние сервисы в карточке уязвимости (NVD, Vulners.com, Exploit-DB, БДУ ФСТЭК)	1. В результатах сканирования провести анализ полноты информации в карточке актива. 2. Проверить достаточность информации в карточке актива для принятия решения по ее устранению.	Решение предоставляет детальную информацию в карточке уязвимости и актива.
6.13	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК	1. В результатах сканирования найти рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК.	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК.
6.14	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ	1. В результатах сканирования найти рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ.	Решение предоставляет рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ.
Оценка соответствия			
7.1	Проверка активов на соответствие предустановленным стандартам защищенной конфигурации	1. Провести сканирование и проверить активы на соответствие стандартам, рекомендации производителей ПО и ОС, внутренние стандарты от вендора). 2. Проанализировать результаты. • По выходным данным можно однозначно оценить: критичность проверки; • результат проверки (соответствие/несоответствие).	Решение позволяет проводить проверку соответствия требованиям.
7.2	Возможность формирования пользовательских проверок для актива	1. Добавить в ранее созданный профиль сканирования кастомные настройки проверки соответствия (наличие/отсутствие определенной записи в файле /etc/hosts). 2. Провести повторное сканирование.	Решение позволяет создавать пользовательские проверки.
7.3	Возможность точечной переоценки по активу	1. Для ранее просканированного актива произвести переоценку.	Решение имеет функционал точечной переоценки по активу.
7.4	Ведение истории оценки соответствия	1. Для актива из существующей проверки на соответствие отобразить историю оценки.	В решении имеется возможность отслеживать историю оценки соответствия.
7.5	Разграничение прав доступа к объектам решения	1. Создать роль, имеющую доступ к информации об уязвимостях одной группы активов.	Решение позволяет ограничивать права доступа к объектам решения.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Оценка соответствия	
7.6	Возможность настройки парольной политики: • настраиваемая сложность пароля (буквы, цифры, заглавные, спецсимволы) • история ранее заданных паролей • минимальная длина паролей • время жизни пароля	1. Настроить требования (буквы, цифры, заглавные, спецсимволы) и проверить принятие/отклонение тестовых паролей. 2. Сменить пароль несколько раз и убедиться, что старые пароли блокируются. 3. Установить минимальную длину пароля (например, 8 символов) и проверить отклонение коротких паролей. 4. Настроить срок действия пароля и убедиться, что система требует смены пароля вовремя.	Настройки парольной политики работают корректно.
7.7	Шифрование критичных данных (в т.ч. с использованием пользовательских ключей шифрования)	1. Получить доступ к БД. 2. Убедиться, что настройки УЗ для сканирований находятся в зашифрованном виде.	Решение хранит настройки в зашифрованном виде, или доступ к ним невозможен.
7.8	Возможность создания и восстановления из резервной копии системы	1. Произвести резервное копирование посредством внутреннего функционала решения. 2. Провести восстановление из резервной копии.	Решение позволяет создавать и восстанавливать из резервной копии системы.
7.9	Принудительная смена паролей	1. Назначить принудительную смену пароля для ранее созданного пользователя. 2. Авторизоваться от имени этого пользователя.	В решении реализована принудительная смена пароля.
7.10	Механизмы блокировки учетных записей после нескольких неудачных попыток входа	1. Настроить блокировку пользователей после 5 неудавшихся авторизаций. 2. Попробовать авторизоваться 5 раз с неверным паролем. 3. Проверить статус этого пользователя в интерфейсе решения.	В решении реализована блокировка пользователей при неудачной авторизации.
		Производительность и эффективность	
8.1	Скорость обнаружения новых уязвимостей: время между появлением новой уязвимости в публичных базах (например, NVD, БДУ ФСТЭК) и ее добавлением в сканер	1. До первичной настройки решения необходимо зафиксировать 5 уязвимостей, опубликованных в день подготовки к тестированию. 2. После выполнения проверки убедиться, что уязвимости появились в базе знаний решения. 3. Если новых уязвимостей нет, то провести повторное обновление через 6 часов и проверить появление уязвимостей. 4. Далее провести проверку через 12 часов и через 24 часа после первого обновления.	Время обнаружения новых уязвимостей зафиксировано и составляет менее 24 часов.
8.2	Настройка интенсивности сканирования	1. Для задачи из ранее настроенной проверки настроить меньшую интенсивность сканирования. 2. Произвести повторное сканирование. 3. Сравнить время сканирования и полноту информации с результатами предыдущей итерации.	Решение имеет функционал настройки интенсивности сканирования.
		Сканирование веб-ресурсов	
9.1	Проверка OWASP Top 10	1. Настроить сканирование веб-приложения на уязвимости. В качестве целей указать серверы с уязвимыми приложениями. 2. Произвести сканирование. 3. Провести проверку результатов на наличие присутствующих уязвимостей.	Решение позволяет выполнять проверку OWASP top 10.
9.2	Обнаружение и тестирование WAF	1. В результатах сканирования веб-ресурса защищаемого WAF проверить, удалось ли решению обнаружить использование WAF.	Решение может обнаруживать и тестировать WAF-решения.

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Сканирование веб-ресурсов	
9.3	Возможность аутентификации для глубокого изучения веб-приложений (cookie, логин-пароль, заголовки и их значения)	1. Настроить УЗ для веб-сканирования из предыдущей проверки. 2. Провести повторное сканирование.	Решение может аутентифицироваться на сайтах при сканировании.
9.4	Сканирование в режиме поиска поддоменов	1. Запустить задачу на сканирование в режиме поиска поддоменов.	Решение имеет функционал сканирования в режиме поиска поддоменов.
9.5	Обработка токенов Anti-CSRF	1. Настроить сканирование цели с настроенным использованием Anti-CSRF токенов. 2. Убедиться, что в результатах сканирования нет ошибок выполнения запросов.	Решение успешно просканировало цель, и наличие токенов не повлияло на результат.
9.6	Сканирование в режиме атаки	1. Произвести сканирование в режиме атаки для сканирования из ранее созданной проверки. 2. Получить результаты эксплуатации уязвимостей. 3. Убедиться, что в результатах доступна информация о полученных данных в ходе эксплуатации уязвимостей (например, ответ веб-сервера).	Решение имеет функционал сканирования ресурсов в режиме атаки.
9.7	Обнаружение уязвимостей типа «Code & Command Injection»	1. В результатах сканирования найти уязвимостей 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».
9.8	Обнаружение уязвимостей, связанных с загрузкой файлов и доступом к файловой системе	1. В результатах сканирования найти уязвимости, связанные с загрузкой файлов и доступом к файловой системе. Например, Remote File Inclusion, Path Traversal, File Upload Vulnerabilities.	Решение обнаруживает уязвимости, связанные с загрузкой файлов и доступом к файловой системе.
9.9	Обнаружение уязвимостей типа «Client-Side Attacks»	1. В результатах сканирования найти уязвимостей типа «Client-Side Attacks». Например, XSS (Cross-Site Scripting), Script ActiveX Object.	Решение обнаруживает уязвимости типа «Client-Side Attacks».
9.10	Обнаружение уязвимостей типа «Redirection & Resource Access»	1. В результатах сканирования найти уязвимости типа «Redirection & Resource Access». Например, Open Redirect (External Redirect), Server Side Request Forgery (SSRF), XML External Entity (XXE), Cross-Domain Misconfiguration (CORS)).	Решение обнаруживает уязвимости типа «Redirection & Resource Access».
9.11	Обнаружение уязвимостей типа «Cryptographic Weaknesses»	1. В результатах сканирования найти уязвимости типа «Cryptographic Weaknesses». Например, Weak Cipher Suite, Heartbleed (OpenSSL)).	Решение обнаруживает уязвимости типа «Cryptographic Weaknesses».
9.12	Обнаружение уязвимостей типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)»	1. В результатах сканирования найти уязвимости типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)». Например, Insecure Referrer Policy Header, Content Security Policy (CSP) Missing, X-Content-Type-Options Header Missing, X-Frame-Options Header Missing, X-Permitted-Cross-Domain-Policies Header Missing, X-XSS-Protection Header Missing, Strict-Transport-Security Header Missing, Incomplete or No Cache-control and Pragma HTTP Header Set.	Решение обнаруживает уязвимости типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)».
9.13	Обнаружение уязвимостей типа «Information Disclosure»	1. 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».
9.14	Обнаружение уязвимостей типа «Cookie Security Issues»	1. В результатах сканирования найти уязвимости типа «Cookie Security Issues». Например, Cookie No HttpOnly Flag, Cookie No Secure Flag.	Решение обнаруживает уязвимости типа «Cookie Security Issues».

№ П/П	КРИТЕРИЙ	ШАГИ ВЫПОЛНЕНИЯ	ОЖИДАЕМЫЕ РЕЗУЛЬТАТЫ
		Сканирование веб-ресурсов	
9.15	Обнаружение уязвимостей типа «Memory Corruption»	1. В результатах сканирования найти уязвимости типа «Memory Corruption». Например, Buffer Overflow, Format String, Integer Overflow.	Решение обнаруживает уязвимости типа «Memory Corruption».
		Документация	
10.1	Предоставлена ли полная и детализированная документация от вендора	Поверить наличие следующей информации в документации вендора: • Описание архитектуры решения. • Требования к ОС. • Требования к аппаратному обеспечению, включая параметры сайзинга (масштабирования) решения. • Описание и достаточность инструкции по инсталляции. По итогу тестирования оценивается, количество дополнительных обращений к вендору/эксперту по моментам, не описанным в инструкции по инсталляции. • Полнота описания инструкции администратора по функционалу решения на соответствие реальному функционалу стенда. Оценивается детализация описанного функционала в инструкции и количество не описанного функционала в документации, который явно присутствует в интерфейсе решения. • Описания способов резервного копирования и восстановления конфигурации и накопленных данных. • Описание настройки способов кластеризации решения и распределения нагрузки (при наличии такого функционала в решении). • Описание закрытых ошибок в версии решения, описание известных ошибок в решении и способов их обхода (release notes).	В документации представлена перечисленная информация.