Инфосистемы Джет

ПОЛНЫЕ РЕЗУЛЬТАТЫ ТЕСТИРОВАНИЯ

ОГЛАВЛЕНИЕ

О ПРОЕКТЕ

Наша инициатива направлена на **формирование детального обзора российских решений для управления уязвимостями**. Мы хотим помочь бизнесу выбрать оптимальные инструменты для своих задач в этой области.

На базе лаборатории «Инфосистемы Джет» мы проводим тестирование доступных в России решений для управления уязвимостями ИБ, беспристрастно и по открытой для всех методологии. Наши эксперты последовательно тестируют решения и делятся новыми результатами на сайте. Рекомендуем подписаться на рассылку или следить за публикациями, чтобы оставаться в курсе изменений.

МЕТОДИКА

Каждое решение мы проверяли по единому сценарию — от обнаружения уязвимостей до формирования отчетов и интеграции с другими системами безопасности.

Мы подобрали критерии на основе нашего опыта работы с заказчиками из различных сфер деятельности: финансы, телекоммуникации, промышленность и государственный сектор. Учли наши экспертные ожидания в области управления уязвимостями, чтобы гарантировать соответствие решений современным требованиям к функционалу и удобству их использования.

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
			Общая организационная информация		
1.1	Автоматическое обновление базы уязвимостей по сети	Да		Да	
1.2	Возможность офлайн-обновления базы уязвимостей сканера	Да		Да	
1.3	Централизованное управление через веб-интерфейс	Да		Да	
1.4	Возможность установки агентов на хосты	Частично	Возможна установка хостовых агентов MP EDR	Да	
1.5	Возможность работы в частично или полностью изолированных сегментах сети	Да		Частично	Поддерживается работа в частично изолированных сетях, поддержка работы в полностью изолированных — планируется в новом продукте RedCheck VM в 2026 году
1.6	Локализация интерфейса и поддержка мультиязычности	Да		Нет	Поддерживается только русский язык
1.7	Наличие сертификата ФСТЭК и присутствие решения в реестре отечественного ПО	Да		Да	
			Управление активами		
2.1	Построение интерактивной карты сети	Да		Нет	
2.2	Создание динамических групп активов	Да		Нет	Планируется в новом продукте RedCheck VM в 2026 году
2.3	Поиск по группам активов	Да		Частично	Есть возможность поиска активов внутри группы по времени обнаружения активов, по IP-адресу/FQDN, CPE и описанию
2.4	Кастомизация карточки актива и уязвимости	Частично	Возможности кастомизировать карточку уязвимости нет	Нет	
2.5	Скоринг активов: расчет уровня критичности	Да		Нет	
2.6	Дедупликация данных об активах	Да		Нет	Планируется в новом продукте RedCheck VM в 2026 году
2.7	Тегирование активов	Нет	Планируется в 2025 году	Нет	
			Настройка общих правил и логики системы		
3.1	Импорт и экспорт профилей и результатов сканирования между инсталляциями в рамках одного решения	Да		Нет	

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
Настройка общих правил и логики системы					
3.2	Встроенный функционал ведения процесса устранения уязвимостей	Да		Частично	Планируется в новом продукте RedCheck VM в 2026 году
3.3	Настройка правил отправки оповещений	Да		Да	
3.4	Поддержка сквозного поиска, фильтрации, сортировки по активам и уязвимостям	Да		Да	
3.5	Функционал патч-менеджмента	Нет	В паспорте уязвимости присутствует ссылка на патч вендора	Нет	
3.6	Настройка правил автоматической смены статуса уязвимости (перерасчета критичности, срока, способа устранения)	Да		Нет	
3.7	Визуализация данных в виде настраиваемых виджетов и дашбордов	Да		Нет	
Поддерживаемые типы активов для сканирования					
4.1	Поддержка сканирования ОС	Да	Протестировано: ОС Windows Server, Windows ARM, AstraLinux, AlmaLinux, Ubuntu, РедОС, Debian	Да	Протестировано: ОС Windows Server, Windows ARM, AstraLinux, AlmaLinux, Ubuntu, РедОС, Debian
4.2	Поддержка сканирования сетевого оборудования	Да	Протестировано: Cisco Nexus, Cisco IOS, Cisco ASA, Huawei ARP	Да	Протестировано: Usergate UTM 6.1.9
4.3	Поддержка сканирования периферийного оборудования	Частично	Поддерживаются только в режиме пентест	Нет	
4.4	Поддержка сканирования ИТ-решений	Да	Протестировано: Microsoft Active Directory, VMware ESXi, СУБД PostgreSQL, СУБД MSSQL, СУБД Oracle, Docker Container	Да	Протестировано: Microsoft Active Directory, VMware ESXi, СУБД PostgreSQL, СУБД MSSQL, СУБД Oracle, Docker Container
4.5	Поддержка сканирования ИБ-решений	Да	Протестировано: Check Point Security Management Server (ОС GAiA)	Да	Протестировано: Check Point Security Management Server (ОС GAiA)
4.6	Инвентаризация и поиск уязвимостей в запущенных контейнерах	Да	Протестировано: Docker Container на ОС Ubuntu	Да	Протестировано: Docker Container на ОС Ubuntu, AstraLinux
Возможности интеграции					
5.1	Наличие документированного API для: a. Получения результатов сканирования (получения активов и уязвимостей) b. Заведение профилей/задач сканирования c. Запуска сканирования	Да		Да	
5.2	Возможность интеграции с системами мониторинга работоспособности	Да		Нет	

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
Возможности интеграции					
5.3	Интеграция с Microsoft Active Directory	Да		Да	
5.4	Интеграция с SIEM	Да	Возможна интеграция с MP SIEM	Да	
Управление сканированием и уязвимостями					
6.1	Расписание сканирований	Да		Да	
6.2	Сканирование в режиме brute force для возможности перебора паролей в целевых системах	Да		Частично	Брутфорс по RDP не поддерживается
6.3	Настройка правил и логики профилей сканирования	Да		Да	
6.4	Настройка сканирования (выбор диапазонов подсетей/IP-адресов/портов)	Да		Да	
6.5	Прогнозирование рисков: возможность оценки потенциального ущерба от эксплуатации уязвимостей	Да		Да	
6.6	Ведение и отображение идентификаторов уязвимостей (CVE, NVD, БДУ, CPE, CWE).	Да		Да	
6.7	Поддержка CVSS-метрик версий 2/3/4 и возможности задания кастомных метрик CVSS	Частично	Поддержка CVSS-метрик версии 4 — планируется в 2025 году	Частично	Кастомные метрики и CVSS-метрики версии 4 отсутствуют
6.8	Поддержка нотации OVAL, возможность добавления собственной проверки уязвимостей	Нет		Да	
6.9	Настраиваемый скоринг уязвимостей	Да	Возможно с использованием PDQL-запросов	Нет	
6.10	Проверка эксплуатируемости уязвимости	Да		Да	
6.11	Дедупликация данных об уязвимостях	Да		Да	
6.12	Ссылки на внешние сервисы в карточке уязвимости (NVD, Vulners.com, Exploit-DB, БДУ ФСТЭК)	Да		Да	
6.13	Рекомендации по устранению выявленных уязвимостей от ФСТЭК	Да		Да	
6.14	Рекомендации по устранению выявленных уязвимостей от НКЦКИ	Да		Да	

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
	Оценка соответствия				
7.1	Проверка активов на соответствие предустановленным стандартам защищенной конфигурации	Да	Используются только встроенные стандарты от вендора	Частично	Присутствуют стандарты CIS, ГОСТ Р 57580.1-2017, PCI DSS, ФСТЭК №239, ФСТЭК №239№31, МД ФСТЭК России от 25.12.2022, ГИС, рекомендации производителей ОС и ПО, встроенные стандарты от вендора
7.2	Возможность формирования пользовательских проверок для актива	Да		Да	
7.3	Возможность точечной переоценки по активу	Да	Переоценка происходит автоматически	Да	
7.4	Ведение истории оценки соответствия	Да		Да	
	Безопасность и надежность				
8.1	Разграничение прав доступа к объектам решения	Да		Нет	Возможно использование только преднастроенных ролей
8.2	Возможность настройки парольной политики - настраиваемая сложность пароля (буквы, цифры, заглавные, спецсимволы) - история ранее заданных паролей - минимальная длина паролей - время жизни пароля	Да		Да	
8.3	Шифрование критичных данных (в т.ч. с использованием пользовательских ключей шифрования)	Частично	Процедурно генерируемый ключ при установке	Да	
8.4	Возможность создания и восстановления из резервной копии системы	Да		Частично	Резервное копирование БД осуществляется средствами СУБД. Восстановление осуществляется путем установки ПО с настройкой к подключению уже существующей БД
8.5	Принудительная смена паролей	Да		Нет	
8.6	Механизмы блокировки учетных записей после нескольких неудачных попыток входа	Да		Нет	
	Производительность и эффективность				
9.1	Скорость обнаружения новых уязвимостей: время между появлением новой уязвимости в публичных базах (например, NVD, БДУ ФСТЭК) и ее добавлением в сканер	Скорость появления зависит от критичности уязвимости. Трендовые уязвимости — в течение 12 часов, остальные — не реже 1 раза в сутки		Время добавления новых уязвимостей в систему — более 24 часов	

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
			Производительность и эффективность		
9.2	Настройка интенсивности сканирования	Да		Да	
			Сканирование веб-ресурсов		
10.1	Проверка OWASP Top 10	Да		Да	
10.2	Обнаружение и тестирование WAF	Нет		Нет	
10.3	Возможность аутентификации для глубокого изучения веб-приложений (cookie, логин-пароль, заголовки и их значения)	Да		Нет	
10.4	Сканирование в режиме поиска поддоменов	Частично	Есть возможность указать в настройках задачи глубину сканирования в части затрагиваемых ресурсов (от проверки только страницы до поиска по всем поддоменам)	Нет	
10.5	Обработка токенов Anti-CSRF	Частично	В зависимости от реализации CSRF динамический токен может мешать сканированию	Нет	
10.6	Сканирование в режиме атаки	Да		Нет	
10.7	Обнаружение уязвимостей типа «Code & Command Injection»	Да		Да	
10.8	Обнаружение уязвимостей, связанных с загрузкой файлов и доступом к файловой системе	Да		Да	
10.9	Обнаружение уязвимостей типа «Client-Side Attacks»	Да		Да	
10.10	Обнаружение уязвимостей типа «Redirection & Resource Access»	Да		Да	
10.11	Обнаружение уязвимостей типа «Cryptographic Weaknesses»	Да		Да	
10.12	Обнаружение уязвимостей типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)»	Да		Да	
10.13	Обнаружение уязвимостей типа «Information Disclosure»	Да		Да	
10.14	Обнаружение уязвимостей типа «Cookie Security Issues»	Да		Да	
10.15	Обнаружение уязвимостей типа «Memory Corruption»	Да		Да	

№ П/П	КРИТЕРИЙ	MAX PATROL VM V.2.8 (27.3)	ПРИМЕЧАНИЕ	REDCHECK V.2.9.1	ПРИМЕЧАНИЕ
Документация					
11.1	Предоставлена ли полная и детализированная документация от вендора	Да		Да	