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	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
Общая организационная информация											
1	Автоматическое обновление базы уязвимостей по сети	Да		Да		Да		Да		Да	
2	Оффлайн обновления базы уязвимостей сканера	Да		Да		Нет	Планируется в Q3 2025	Да		Да	
3	Открытый доступ к базе уязвимостей в продукте	Да		Да		Нет		Да		Да	
4	Централизованное управление через веб-интерфейс	Да		Да		Да		Да		Да	
5	Возможность установки агентов на хосты	Да		Да		Нет		Частично	Поддерживается установка агентов только на Windows-активы	Да	
6	Возможность обновления агентов встроенным механизмом продукта	Да		Да		Нет		Нет		Да	
7	Возможность работы в частично или полностью изолированных сегментах сети	Да		Да		Частично	Имеется возможность работы в частично изолированных сегментах сети путем развертывания дополнительных нод сканирования	Частично	Поддерживается работа в частично изолированных сетях, поддержка работы в полностью изолированных сегментах сети - планируется в новом продукте RedCheck VM в 2026 году	Частично	Работа в изолированном сегменте возможна, но информацию об оффлайн активах необходимо передавать через API
8	Поддержка мультиязычности	Да		Да		Да		Нет	Поддерживается только русский язык	Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
9	Наличие сертификата ФСТЭК и присутствие решения в реестре отечественного ПО	Да		Да		Частично	Сертификат ФСТЭК на ПО отсутствует	Да		Частично	Присутствует в реестре отечественного ПО. Подана заявка на получение сертификата ФСТЭК
10	Возможность поставки от производителя в виде программно-аппаратного комплекса	Нет		Да		Да		Нет		Да	
Управление активами											
11	Построение интерактивной карты сети	Да		Да		Нет		Нет		Нет	
12	Создание динамических групп активов	Да		Да	Реализовано через настройку рабочих процессов	Нет		Нет	Планируется в новом продукте RedCheck VM в 2026 году	Да	
13	Поиск по группам активов	Да		Да		Да		Частично	Поддерживается поиск активов внутри группы по времени обнаружения активов, по IP-адресу/FQDN, CPE и описанию	Да	
14	Кастомизация карточки актива	Да		Да		Нет		Нет		Нет	Планируется в Q3 2025
15	Скоринг активов: расчет уровня критичности	Да		Да		Нет	Планируется в Q4 2025	Нет		Да	
16	Дедупликация данных об активах	Да		Да		Да		Нет	Планируется в новом продукте RedCheck VM в 2026 году	Нет	При импорте активов из AD/LDAP имеется возможность исключить уже существующие в системе активы

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
17	Создание пользовательских отметок (тегов)	Нет	Планируется в 2025 году	Да		Да		Нет		Да	
18	Хранение истории изменения актива	Да		Да		Да		Частично	Доступна история результатов сканирования актива и имеется возможность создания дифференциальных отчетов	Да	
19	Запуск административных действий/команд, выполняемых на активах	Да	Для Linux доступно только в рамках запуска задачи на сканирование	Да		Нет		Нет		Да	
Настройка общих правил и логики системы											
20	Импорт и экспорт политик и результатов сканирования между инсталляциями в рамках одного решения	Да		Да		Нет		Нет		Нет	Возможен экспорт данных в формате json из интерфейса и при помощи методов API
21	Создание и управление задачами на устранение уязвимостей	Нет		Да		Нет		Нет	Планируется в новом продукте RedCheck VM в 2026 году	Да	
22	Назначение ответственных для задачи на устранение уязвимостей	Нет		Да		Нет		Нет	Планируется в новом продукте RedCheck VM в 2026 году	Да	
23	Настройка правил отправки оповещений о сканированиях	Да		Да		Да		Да		Нет	
24	Поддержка сквозного поиска, фильтрации, сортировки по активам и уязвимостям	Да		Да		Частично	Сортировка отсутствует	Да		Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
25	Функционал патч-менеджмента	Нет		Да		Нет		Нет		Да	
26	Автоматизация управления параметрами уязвимости (например, перерасчет критичности, срока, способа устранения)	Да		Да		Нет	Имеется возможность поставить статус уязвимости вручную	Нет	Планируется в новом продукте RedCheck VM в 2026 году	Нет	
27	Визуализация данных в виде настраиваемых виджетов и дашбордов	Да		Да		Нет		Нет		Нет	
28	Возможность создания и экспорта пользовательских отчетов	Да		Да		Нет		Частично	Предусмотрен набор фильтров для предустановленных отчетов	Нет	Планируется в Q4 2025
29	Выпуск отчетов по расписанию	Да		Да		Да		Нет	Отчеты направляются только по окончании выполнения сканирования	Да	
Поддерживаемые типы активов для сканирования											
30	Поддержка сканирования ОС: Windows Server, Windows ARM, Astra Linux, Alma Linux, Ubuntu, РедОС, Debian	Да		Да		Частично	РедОС не поддерживается	Да		Да	
31	Поддержка сканирования сетевого оборудования	Да		Да		Да		Да		Да	
32	Поддержка идентификации периферийных устройств (например, камеры, IP-телефония, принтеры)	Да		Да		Да		Да		Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
33	Поддержка сканирования СУБД (например, Oracle, PostgreSQL, MSSQL)	Да		Да		Да		Да		Частично	Не поддерживается создание задач на аудит СУБД. Уязвимости в СУБД обнаруживаются при аудите ОС
34	Поддержка сканирования серверного ПО (например, веб-серверы, службы каталогов, почтовые сервера, системы виртуализации)	Да		Да		Да		Да		Да	
35	Сканирование промышленных систем управления (ICS/SCADA)	Да		Да		Да		Да		Да	
36	Инвентаризация и поиск уязвимостей в контейнерах	Да		Да		Нет		Да		Да	
Возможности интеграции											
37	Наличие документированного API	Да		Да		Да		Да		Да	Документация предоставляется по запросу. Оформлена в виде Swagger
38	Разграничение доступа для API-ключей	Да		Да		Да		Да		Да	
39	Возможность интеграции с системами мониторинга работоспособности	Да	Настраивается на стороне встроенной Grafana	Да		Да		Нет		Нет	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.174896 8449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
40	Поддержка доменной авторизации	Да		Да		Да		Да	Для доменной авторизации необходимо включить сервер RedCheck в домен и создать keytab-файл	Да	
41	Интеграция с Service Desk/ITSM системами	Нет		Да		Нет	Выгрузка данных доступна через интеграцию с бесплатной community-версией SGRC Securitm	Нет		Да	
42	Интеграция с SIEM в части отправки событий	Нет		Да		Нет		Да		Нет	
43	Функционал получения данных об активах из смежных систем (например, из службы каталогов, среды виртуализации, SIEM-системы, смежных сканеров)	Да	Импорт из AD, среды виртуализации, MaxPatrol SIEM	Да	Поддерживается большое количество интеграций с внешними системами, включая возможность создания коннекторов к новым системам	Нет	Выгрузка данных доступна через интеграцию с бесплатной community-версией SGRC Securitm	Да	Импорт из AD, FreeIPA и ALD	Да	Импорт из AD, LDAP и реестра докеров
Управление сканированием и уязвимостями											
44	Кастомизация карточки уязвимости	Нет		Да		Нет		Нет		Нет	
45	Расписание сканирований	Да		Да		Да		Да		Да	
46	Поиск уязвимостей без повторного сканирования хостов (ретро-скан)	Да		Да		Нет		Нет		Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
47	Настройка "технологических окон" для активов	Нет	Поддерживается настройка "технологических окон" в задачах на сканирование	Да		Да		Нет	Поддерживается настройка "технологических окон" в задачах на сканирование	Да	
48	Сканирование в режиме brute force для возможности перебора паролей в целевых системах	Да		Да		Да		Частично	Сканирование в режиме "brute force" по RDP не поддерживается	Нет	
49	Настройка правил и логики профилей сканирования	Да		Да		Да		Да		Да	
50	Настройка сканирования (выбор диапазонов подсетей/IP-адресов/портов)	Да		Да		Да		Да		Частично	Поддерживается сканирование только уже добавленных активов. Сканирование подсетей планируется к реализации в Q4 2025
51	Добавление исключений при сканировании (например, уязвимость, порт, ПО)	Частично	Все исключения можно добавлять в отчеты при помощи PDQL-запросов. В профиле сканирования есть возможность исключать ПО из аудита	Да		Да		Частично	Возможность добавлять исключения есть только в рамках создания отчетов	Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.174896 8449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
52	Описание последствий эксплуатации уязвимости в карточке	Да		Да		Да		Да		Да	
53	Ведение и отображение идентификаторов уязвимостей (CVE, NVD, БДУ, CPE, CWE).	Да		Да		Да		Да		Да	
54	Поддержка CVSS-метрик версий 2/3/4 и возможности задания кастомных метрик CVSS	Частично	Поддержка CVSS v4 планируется в 2025 году	Да		Частично	Для разных типов сканеров используются разные метрики CVSS (если их использует данный тип сканера). Возможность задания кастомных метрик CVSS отсутствует	Частично	Кастомные метрики отсутствуют	Частично	Отсутствует возможность задать кастомную метрику
55	Добавление собственной проверки уязвимостей	Нет		Да		Нет	Планируется в начале Q4 2025	Да	Поддержка OVAL-определений, пользовательских YARA-правил и LUA-скриптов для кастомного поиска угроз	Нет	
56	Настраиваемый скоринг уязвимостей	Да		Да		Да		Нет		Нет	
57	Проверка эксплуатируемости уязвимости	Да		Да		Да		Да		Да	
58	Дедупликация данных об уязвимостях	Да		Да		Да		Да		Да	
59	Ссылки на внешние сервисы в карточке уязвимости (NVD, Vulners.com, Exploit-DB, БДУ ФСТЭК)	Да		Да		Да		Да		Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
60	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от ФСТЭК	Да		Да		Нет		Да		Да	
61	Рекомендации по устранению уязвимости на основе выявленных уязвимостей от НКЦКИ	Да		Да		Нет		Да		Да	
62	Расчет критичности уязвимости по методике ФСТЭК	Да	Оценка не отображается в карточке актива. Требуется использовать подготовленный PDQL-запрос	Да		Нет		Нет	Планируется в новом продукте RedCheck VM в 2026 году	Да	
63	Проверка обновлений Windows (KB) по БДУ ФСТЭК	Нет		Да		Нет		Нет		Да	
64	Оповещения о событиях в Системе (например, появления нового актива, важной уязвимости на активе, обновление базы уязвимостей)	Да		Да		Да	Поддерживается только оповещения о найденных уязвимостях	Да	Поддерживаются только отправка уведомлений об обновлении базы уязвимостей и уведомление об окончании выполнения задачи	Нет	Планируется в 2026
Оценка соответствия											
65	Проверка активов на соответствие предустановленным стандартам защищённой конфигурации	Да		Да		Да		Да		Нет	Планируется в 2026
66	Формирование пользовательских проверок для актива	Да		Да		Нет	Планируется в начале Q4 2025	Да		Нет	Планируется в 2026

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
67	Точечная переоценка по активу	Да		Да		Да		Да		Нет	Планируется в 2026
68	Ведение истории оценки соответствия	Да		Да		Нет		Да		Нет	Планируется в 2026
	Безопасность и надежность										
69	Разграничение прав доступа к объектам решения	Да		Да		Да		Нет	Поддерживается использование только преднастроенных ролей	Нет	Планируется в 2026
70	Возможность настройки парольной политики - настраиваемая сложность пароля (буквы, цифры, заглавные, спецсимволы) - история ранее заданных паролей - минимальная длина паролей - время жизни пароля	Да		Да		Да		Нет	Поддерживается настройка средствами Active Directory при настроенной доменной авторизации	Частично	Имеется возможность задать историю и срок жизни пароля. Сложность пароля предустановлена на основе требований ФСТЭК
71	Шифрование критичных данных (в т.ч. с использованием пользовательских ключей шифрования)	Частично	Используется процедурно сгенерированный ключ при установке	Частично	Отсутствует функционал использования пользовательских ключей	Да		Да		Частично	УЗ хранятся в HashiCorp Vault. Функционал использования пользовательских ключей шифрования не предусмотрен

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
72	Создание и восстановления из резервной копии системы	Да		Частично	Доступно резервное копирование средствами СУБД или средствами docker	Нет		Частично	Резервное копирование БД осуществляется средствами СУБД. Восстановление RedCheck осуществляется путем установки ПО с настройкой к подключению уже существующей БД	Да	
73	Принудительная смена паролей	Да		Да		Да		Нет		Да	
74	Механизмы блокировки учетных записей после нескольких неудачных попыток входа	Да		Да		Да		Нет	Поддерживается средствами Active Directory при настроенной доменной авторизации	Да	
75	Интеграция с системами хранения секретов в части хранения учетных записей для сканирования (например, HashiCorp Vault)	Нет		Да		Нет		Нет		Да	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
Производительность и эффективность											
76	Скорость обнаружения новых уязвимостей: Время между появлением новой уязвимости в публичных базах (например, NVD, БДУ ФСТЭК) и её добавлением в сканер	Скорость появления зависит от критичности уязвимости. Трендовые уязвимости — в течение 12 часов, остальные — не реже 1 раза в сутки		Время между появлением уязвимости и добавлением ее в базу примерно 48 часов		24 часа		Время добавления новых уязвимостей в Систему примерно 72 часа		3 часа	
77	Настройка интенсивности сканирования	Да		Частично	Реализуется путем настройки конфигурационных файлов сервисов, имеется возможность настроить получение значений в справочнике с возможностью редактирования значения.	Да		Да		Частично	На стороне сервера настраивается количество контейнеров, выявляющих уязвимости по получаемым данным с активов. Для сканирования в режиме черного ящика настройка реализована на уровне задачи

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.174896 8449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
78	Поддержка сканирования георасределенных филиалов, мультитенантность	Частично	Поддержка мультитенантности - планируется в 2026 году	Да		Частично	В рамках одной инсталляции возможно создание нескольких независимых "Личных кабинетов". Централизованное управление ими отсутствует	Да	Поддерживается сегментная ролевая модель для разделения хостов и задач между пользователями	Да	
Сканирование веб-ресурсов											
79	Проверка OWASP Top 10	Да		Да		Да		Да		Нет	
80	Обнаружение WAF	Нет		Да		Да		Нет		Нет	
81	Возможность аутентификации для глубокого изучения веб-приложений (cookie, логин-пароль, заголовки и их значения)	Да		Нет	Планируется в Q4 2025	Да		Нет		Нет	
82	Сканирование в режиме поиска поддоменов	Частично	Имеется возможность указать в настройках задачи глубину сканирования в части затрагиваемых ресурсов (от проверки только страницы до поиска по всем поддоменам)	Нет	Планируется в Q4 2025	Да		Нет		Нет	
83	Поиск скрытых файлов и папок (dirsearch)	Нет		Да		Да		Нет		Нет	
84	Обнаружение уязвимостей типа «Cross-Site Request Forgery»	Нет		Да		Да		Да		Нет	

№ П/П	КРИТЕРИЙ	MAXPATROL VM V 2.8 (27.3)	ПРИМЕЧАНИЕ	SECURITY VISION V.5.0.1748968449	ПРИМЕЧАНИЕ	SCANFACTORY V.6.12.55	ПРИМЕЧАНИЕ	REDCHECK V.2.11	ПРИМЕЧАНИЕ	VULNS.IO ENTERPRISE VM V 1.35.3	ПРИМЕЧАНИЕ
85	Сканирование в режиме атаки	Да		Да		Да		Нет		Нет	
86	Обнаружение уязвимостей типа «Code & Command Injection»	Да		Да		Да		Да		Нет	
87	Обнаружение уязвимостей, связанных с загрузкой файлов и доступом к файловой системе	Да		Да		Да		Да		Нет	
88	Обнаружение уязвимостей типа «Client-Side Attacks»	Да		Да		Да		Да		Нет	
89	Обнаружение уязвимостей типа «Redirection & Resource Access»	Да		Да		Да		Да		Нет	
90	Обнаружение уязвимостей типа «Cryptographic Weaknesses»	Да		Да		Да		Да		Нет	
91	Обнаружение уязвимостей типа «Отсутствие или неправильная настройка заголовков безопасности (Security Headers)»	Да		Да		Да		Да		Нет	
92	Обнаружение уязвимостей типа «Information Disclosure»	Да		Да		Да		Да		Нет	
93	Обнаружение уязвимостей типа «Cookie Security Issues»	Да		Да		Да		Да		Нет	
94	Обнаружение уязвимостей типа «Memory Corruption»	Да		Да		Да		Да		Нет	