

The Kaspersky logo is displayed in a bold, black, lowercase sans-serif font. It is positioned within a white, irregularly shaped area that resembles a torn piece of paper, set against a background with a green-to-teal gradient and abstract white shapes.

kaspersky

Информация о выпуске Kaspersky Vulnerability Management 1.0

© 2026 АО "Лаборатория Касперского"

Содержание

[Kaspersky Vulnerability Management 1.0](#)

Информация о выпуске Kaspersky Vulnerability Management 1.0

Kaspersky Vulnerability Management (далее также "решение") предназначено для управления уязвимостями в ИТ-инфраструктуре организации.

Kaspersky Vulnerability Management выполняет следующие функции:

- Предоставляет информацию об активах ИТ-инфраструктуры организации.
- Выполняет поиск уязвимостей на активах.
- Выполняет анализ соответствия активов внутренним, отраслевым и регуляторным требованиям безопасности.
- Предоставляет возможности для анализа и приоритизации найденных уязвимостей.
- Предоставляет возможность сторонним системам получать данные об активах и найденных уязвимостях с помощью публичного API.

АППАРАТНЫЕ И ПРОГРАММНЫЕ ТРЕБОВАНИЯ

Минимальные аппаратные требования

Минимальные аппаратные требования к устройству, на котором планируется установка компонентов Kaspersky Vulnerability Management, перечислены в таблице ниже.

Минимальные аппаратные требования

Количество активов	Вариант установки	
	Все на одном устройстве Компоненты Kaspersky Vulnerability Management, включая СУБД, и компоненты Kaspersky Security Center установлены на одном устройстве.	Kaspersky Vulnerability Management отдельно Компоненты Kaspersky Vulnerability Management, включая СУБД, установлены отдельно от компонентов Kaspersky Security Center.
1-1000	• Процессор: 16 ядер, 2,5 ГГц. • Оперативная память: 24 ГБ. • Объем свободного места на диске: 300 ГБ. • Производительность диска, IOPS: 1000.	• Процессор: 12 ядер, 2,5 ГГц. • Оперативная память: 16 ГБ. • Объем свободного места на диске: 200 ГБ. • Производительность диска, IOPS: 1000.
1001-10000	• Процессор: 20 ядер, 2,5 ГГц. • Оперативная память: 48 ГБ. • Объем свободного места на диске: 600 ГБ. • Производительность диска, IOPS: 1000.	• Процессор: 16 ядер, 2,5 ГГц. • Оперативная память: 32 ГБ. • Объем свободного места на диске: 400 ГБ. • Производительность диска, IOPS: 1000.

Программные требования

Компоненты Kaspersky Vulnerability Management могут быть установлены на устройстве под управлением одной из следующих операционных систем:

- Альт Сервер 10 64-разрядная.
- РЕД ОС 8.0 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.

Операционная система в режиме замкнутой программной среды не поддерживается.

- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5) 64-разрядная, в том числе в режиме замкнутой программной среды.
- Debian 11.0 64-разрядная.
- Platform V SberLinux OS Server (SLO) 8.10.1 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.5.1 64-разрядная.
- Ubuntu Server 22.04 LTS 64-разрядная.

Агент администрирования Kaspersky Security Center поддерживает функциональность Kaspersky Vulnerability Management в следующих операционных системах:

- Альт Сервер 10 64-разрядная.
- РЕД ОС 8.0 64-разрядная.
- Astra Linux Common Edition (очередное обновление 2.12) 64-разрядная.
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5) в режиме замкнутой программной среды 64-разрядная.
- Red Hat Enterprise Linux Server 10.0 64-разрядная.
- Rocky Linux 9.6 64-разрядная.
- Ubuntu Server 22.04 LTS 64-разрядная.
- Ubuntu Server 24.04 LTS 64-разрядная.
- Windows 10 32-разрядная/64-разрядная.
- Windows 11 25H2 64-разрядная.
- Windows Server 2025 64-разрядная.

База данных решения может быть создана в одной из следующих СУБД:

- PostgreSQL версии 15.0, 16.0, 17.0, 18.4.
- Postgres Pro 18.4.
- Postgres Pro Certified 18.4.

Поддерживаемые версии Kaspersky Security Center и Агента администрирования

Текущая версия Kaspersky Vulnerability Management поддерживает работу с Сервером администрирования Kaspersky Security Center Linux, Kaspersky Security Center Web Console и Агентом администрирования версии 16.3.

Текущая версия Kaspersky Vulnerability Management не поддерживает работу с Сервером администрирования Kaspersky Security Center Linux, установленным как отказоустойчивый кластер.

Аппаратные и программные требования для Сервера администрирования Kaspersky Security Center, Kaspersky Security Center Web Console и Агента администрирования см. в [справке Kaspersky Security Center](#).

РАЗВЕРТЫВАНИЕ РЕШЕНИЯ

О разворачивании Kaspersky Vulnerability Management читайте в [Справке решения](#).

ИЗВЕСТНЫЕ ОГРАНИЧЕНИЯ

Kaspersky Vulnerability Management имеет ряд не критичных для работы решения ограничений:

- Для некоторых уязвимостей, обнаруженных в результате выполнения задачи *Безагентное сканирование в режиме черного ящика*, отображается только ограниченная информация.
- Не поддерживаются копирование, перемещение, приостановка и возобновление задач Kaspersky Vulnerability Management.
- Результаты выполнения задачи *Безагентное сканирование в режиме черного ящика* отображаются после обработки службой фоновых задач, это занимает некоторое время. Вы можете ускорить обработку результатов, включив функцию **Обрабатывать результаты сразу после завершения задачи** в дополнительных параметрах задачи.
- В карточках приложений, установленных на активах под управлением операционных систем Linux, на вкладке **Установлено на активах** не заполняется поле **Путь к файлу**.
- Не поддерживаны группы активов для формирования области сбора данных для отчетов.

- Область действия роли для Kaspersky Vulnerability Management не ограничена, даже если в области действия роли добавлены комбинации групп администрирования и пользователей.
- Если сессия работы с Kaspersky Vulnerability Management активна и изменен набор прав для учетной записи пользователя этой сессии, изменения вступают в силу с задержкой до пяти минут с момента их внесения.
- В свойствах задач Kaspersky Vulnerability Management на вкладке **Результаты** для событий о статусе задачи *Завершена с предупреждением* не заполняется поле **Описание**.
- Сканирование в режиме белого ящика возможно только на активах под управлением операционных систем семейства Linux.
- При проверке актива под управлением РЕД ОС на соответствие профилям, где есть правило, проверяющее отключение службы автоматического монтирования файловых систем autofs (например, Профиль ФСТЭК России №239 для ОС RedOS и ALT Linux), могут появляться сообщения об ошибке или выдаваться неверные результаты проверки.
- Не работает экспорт отчетов при количестве записей более одного миллиона. Для решения проблемы мы рекомендуем уменьшать число полей (столбцов) в отчете.
- При запуске компонентов Kaspersky Vulnerability Management база данных решения должна быть доступна. В противном случае, компоненты решения не могут запуститься. Для решения этой проблемы следует дождаться, когда база данных решения будет готова принимать соединения, и запустить компоненты решения с помощью команды `sudo /opt/kaspersky/vulnerability-management/helper/helper.sh start`.
- В процессе выполнения задачи *Безагентное сканирование в режиме белого ящика* служба фоновых задач может потреблять много оперативной памяти, если сканируемые активы заражены и чрезмерно отвечают на попытки подключения к ним. Для снижения вероятности исчерпания памяти рекомендуем в настройках задачи не включать в список для сканирования активы, которые вы можете проверить на уязвимости с помощью других типов сканирования, или снизить периодичность выполнения задачи.
- При вызове справки из разделов Kaspersky Vulnerability Management открывается стартовая страница справки, а не соответствующая контексту.
- Поля **Название уязвимости**, **Описание** и **Рекомендации по устранению** отображаются на языке интерфейса Kaspersky Security Center Web Console, который использовался при создании отчета. Если язык интерфейса изменить, эти поля останутся на прежнем языке.

ИСПРАВЛЕННЫЕ ОШИБКИ

Ниже перечислены ошибки, обнаруженные в Kaspersky Vulnerability Management версии 1.0 и исправленные в версии 1.0.1:

- Исправлена ошибка, из-за которой в мастере создания шаблона отчетов и в свойствах шаблона отчетов в разделе **Представление данных** нельзя было перетаскивать строки таблицы.
- Исправлена ошибка, из-за которой в карточке актива на вкладке **Обнаруженные уязвимости** не удалялись записи об уязвимостях, обнаруженных с помощью безагентного сканирования в режиме черного ящика, далее устраненных и повторно просканированных.