

The Kaspersky logo is displayed in a bold, lowercase, sans-serif font. It is positioned within a white, rounded rectangular area that is centered on a background with a green-to-teal gradient and abstract, flowing shapes.

kaspersky

Kaspersky Vulnerability Management 1.1

© 2026 АО "Лаборатория Касперского"

Содержание

[Знакомство с Kaspersky Vulnerability Management](#)

[Что нового в версии 1.1](#)

[Аппаратные и программные требования](#)

[Архитектура решения](#)

[Комплект поставки](#)

[Интерфейс решения](#)

[Поддерживаемые операционные системы](#)

[Поддерживаемое программное обеспечение](#)

[Поддерживаемые профили соответствия](#)

[Подготовка к работе](#)

[Подготовка к развертыванию](#)

[Установка Сервера администрирования Kaspersky Security Center Linux](#)

[Установка Kaspersky Security Center Web Console](#)

[Установка веб-плагина для управления решением](#)

[Создание учетных записей пользователей и настройка доступа по ролям](#)

[Создание и настройка базы данных решения в PostgreSQL](#)

[Установка Агента администрирования Kaspersky Security Center](#)

[Установка утилиты jq](#)

[Установка OpenSSL для Linux](#)

[Установка прочих необходимых утилит](#)

[Применение ключа решения kaspersky_astra_pub_key.gpg](#)

[Развертывание](#)

[Установка и настройка компонентов Kaspersky Vulnerability Management](#)

[Перезапуск службы Kaspersky Security Center Web Console Plugin](#)

[Включение решения на Сервере администрирования](#)

[Включение решения в Агентах администрирования активов](#)

[Работа с активами](#)

[Инвентаризация активов](#)

[Изменение значимости активов](#)

[Работа с группами активов](#)

[Инвентаризация программного обеспечения](#)

[Настройка и выполнение сканирования](#)

[О типах сканирования](#)

[Создание и настройка задач сканирования](#)

[Безагентное сканирование активов в режиме белого ящика](#)

[Безагентное сканирование активов в режиме черного ящика](#)

[Поиск уязвимостей в системном и прикладном ПО](#)

[Сканирование активов на соответствие профилям](#)

[Импорт пользовательских профилей соответствия](#)

[Примеры выбора типа сканирования для разных частей инфраструктуры](#)

[Анализ и приоритизация уязвимостей](#)

[Просмотр найденных уязвимостей](#)

[Работа с отчетами](#)

[Создание и редактирование шаблонов отчетов](#)

[Формирование отчетов на основе шаблонов](#)

[Экспорт отчетов](#)

[Удаление отчетов и шаблонов отчетов](#)

[Работа с данными отчетов](#)

[Сценарий: приоритизация уязвимостей с учетом значимости активов](#)

[Устранение уязвимостей](#)

[Контроль устранения уязвимостей](#)

[Администрирование](#)

[Известные ограничения](#)

[Обновление с версии 1.0 до версии 1.1](#)

[Установка веб-плагина для управления решением](#)

[Обновление баз уязвимостей](#)

[Настройка источника для обновления баз уязвимостей](#)

[Изменение периодичности обновления баз уязвимостей](#)

[Загрузка баз уязвимостей с помощью Kaspersky Update Utility](#)

[Расширенная настройка решения с помощью конфигурационных файлов](#)

[privateapi.json](#)

[publicapi.json](#)

[scanner.json](#)

[updater-compliance.json](#)

[updater-scanner.json](#)

[vms.json](#)

[worker.json](#)

[Использование помощника по настройке](#)

[Разделение доступа к функциям решения по пользовательским ролям](#)

[Создание пользовательских профилей соответствия](#)

[Требования к XCCDF-файлу](#)

[Требования к OVAL-файлам](#)

[Пример XCCDF- и OVAL- файла](#)

[Журналирование событий](#)

[Журнал событий системного аудита](#)

[Журналы событий компонентов решения](#)

[Проверка целостности модулей Kaspersky Vulnerability Management](#)

[Удаление решения](#)

[Выключение Kaspersky Vulnerability Management в Агентах администрирования активов](#)

[Выключение Kaspersky Vulnerability Management на Сервере администрирования](#)

[Удаление компонентов Kaspersky Vulnerability Management](#)

[Удаление веб-плагина для управления решением](#)

[Работа с публичным API решения](#)

[Обращение в Службу технической поддержки](#)

[Источники информации о решении](#)

[Юридическая информация](#)

[Лицензирование решения](#)

[Предоставление данных](#)

[Информация о стороннем коде](#)

[Уведомления о товарных знаках](#)

[Глоссарий](#)

[kvm-group](#)

[OVAL](#)

[XCCDF](#)

[Вероятность EPSS](#)

[Группа администрирования](#)

[Групповая задача](#)

[Приоритет устранения уязвимости](#)

[Профиль соответствия](#)

[Процентиль EPSS](#)

[Сервер администрирования](#)

[Уровень опасности уязвимости](#)

[Уязвимость](#)

Знакомство с Kaspersky Vulnerability Management

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.](#)

Для поддержки решения в актуальном состоянии реализовано регулярное [обновление баз](#).

[Управление решением](#) осуществляется с помощью Kaspersky Security Center Web Console.

Функциональность обновлений и KSN может быть недоступна в решении на территории США.

Что нового в версии 1.1

В Kaspersky Vulnerability Management версии 1.1 появились следующие возможности и доработки:

- Модули Kaspersky Vulnerability Management теперь автоматически проверяются на целостность при запуске. Проверку целостности модулей можно запустить вручную.
- Базы уязвимостей теперь можно обновлять с помощью Kaspersky Update Utility.
- Решение теперь собирает и отображает инвентарную информацию о производителе и версии прошивок материнских плат, выполняет поиск уязвимостей в прошивках.
- Для каждой найденной уязвимости теперь рассчитываются оценки CVSSv2, CVSSv3, CVSSv4. При расчете учитываются базовые и временные метрики, а также данные от поставщика.
- Содержимое полей карточки уязвимости **Название уязвимости**, **Описание** и **Рекомендации по устранению** теперь доступно на русском и английском языках. Язык описания соответствует выбранному языку Kaspersky Security Center Web Console.
- Обновлен список операционных систем, в которых можно установить компоненты Kaspersky Vulnerability Management и Агент администрирования Kaspersky Security Center с поддержкой функций решения.

- Расширен список СУБД, с которыми может работать решение.
- Обновлено списки операционных систем и программного обеспечения, которые поддерживаются в базах уязвимостей решения.

Аппаратные и программные требования

В этой статье указаны версии программного обеспечения, на которых решение было протестировано и для которых гарантируется его корректная работа. Решение также может работать с другими версиями программного обеспечения, но такие конфигурации не проходили полного цикла тестирования и не входят в список гарантированно поддерживаемых.

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.
10001-20000	- Процессор: 24 ядра, 2,5 ГГц. - Оперативная память: 64 ГБ. - Объем свободного места на диске: 1000 ГБ. - Производительность диска, IOPS: 1000.	- Процессор: 20 ядер, 2,5 ГГц. - Оперативная память: 48 ГБ. - Объем свободного места на диске: 600 ГБ. - Производительность диска, IOPS: 1000.

Аппаратные требования для этого количества активов рассчитаны только для задачи Поиск уязвимостей и не учитывают нагрузку от других задач Kaspersky Vulnerability Management.

Программные требования

[Компоненты Kaspersky Vulnerability Management](#) могут быть установлены на устройстве под управлением одной из следующих операционных систем:

- Альт Рабочая станция 11.2 ARM 64-разрядная.
- Альт Сервер 11.0 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Альт СП Сервер 10 64-разрядная.
- РЕД ОС 8.0 64-разрядная.
- РЕД ОС 8.0 Сертифицированная редакция 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 13.0 64-разрядная.
- Platform V SberLinux OS Server (SLO) 9.6 64-разрядная.
- Ubuntu Server 24.04 LTS 64-разрядная.
- Ubuntu Server 26.04 LTS 64-разрядная.

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

- Альт Сервер 10 64-разрядная.
- Альт Сервер 11.0 64-разрядная.
- Альт 8 СП 8.4 Сервер (ЛКНВ.11100-01) 64-разрядная, сертифицированная ФСТЭК России.
- Альт СП Сервер 10 64-разрядная.
- Альт СП Рабочая станция 10 64-разрядная.
- Альт Рабочая станция 11.2 ARM 64-разрядная.
- РЕД ОС 8 64-разрядная.
- РЕД ОС 8.0 Сертифицированная редакция 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.
- Debian 11.0 64-разрядная.
- Debian 13.0 64-разрядная.
- Rocky Linux 9.6 64-разрядная.
- Ubuntu Server 22.04 LTS 64-разрядная.
- Ubuntu Server 24.04 LTS 64-разрядная.
- Ubuntu Server 26.04 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 версии 15.x, 16.x, 17.x, 18.4.
- Postgres Pro Enterprise Certified версии 15.x, 16.x, 17.x, 18.4.
- Platform V Pangolin DB 7.2.0.

Поддерживаемые версии компонентов Kaspersky Security Center

Текущая версия Kaspersky Vulnerability Management поддерживает работу с версией 17 следующих компонентов: Сервер администрирования Kaspersky Security Center Linux, Kaspersky Security Center Web Console и Агент администрирования.

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](#).

Архитектура решения

Kaspersky Vulnerability Management – решение, представляющее из себя совокупность компонентов Kaspersky Vulnerability Management, которые взаимодействуют с компонентами Kaspersky Security Center Linux (далее также "Kaspersky Security Center").

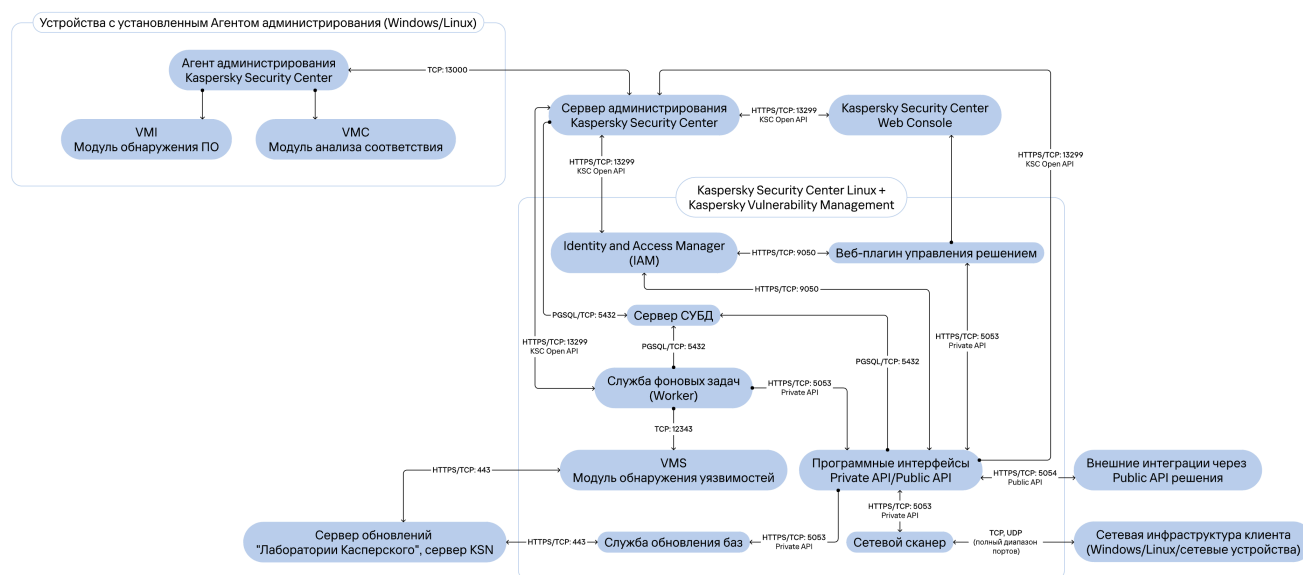
Компоненты Kaspersky Security Center, с которыми взаимодействуют компоненты Kaspersky Vulnerability Management:

- **Сервер администрирования Kaspersky Security Center.** Осуществляет функции централизованного хранения информации об установленных в сети организации приложениях и управления ими.
- **Kaspersky Security Center Web Console.** Представляет собой веб-интерфейс для создания и управления системой защиты сети организации-клиента, находящейся под управлением Kaspersky Security Center.
- **Агент администрирования Kaspersky Security Center.** Обеспечивает взаимодействие между устройствами, на которых он установлен, компонентами Kaspersky Vulnerability Management и Сервером администрирования Kaspersky Security Center (далее также "Сервером администрирования"); участвует в инвентаризации ПО и сканировании активов на соответствие профилям.
- **Identity and Access Manager (IAM).** Компонент Сервера администрирования, позволяющий использовать доменную аутентификацию (единый вход). Функция единого входа позволяет пользователю включить безопасную аутентификацию в Kaspersky Security Center Web Console без повторного ввода пароля в корпоративной сети.
- **Веб-плагин управления решением через Kaspersky Security Center Web Console.** После установки плагина в главном меню Kaspersky Security Center Web Console появляется раздел **Управление уязвимостями**, а также функциональность Kaspersky Vulnerability Management, встроенная в некоторые другие разделы Kaspersky Security Center Web Console.

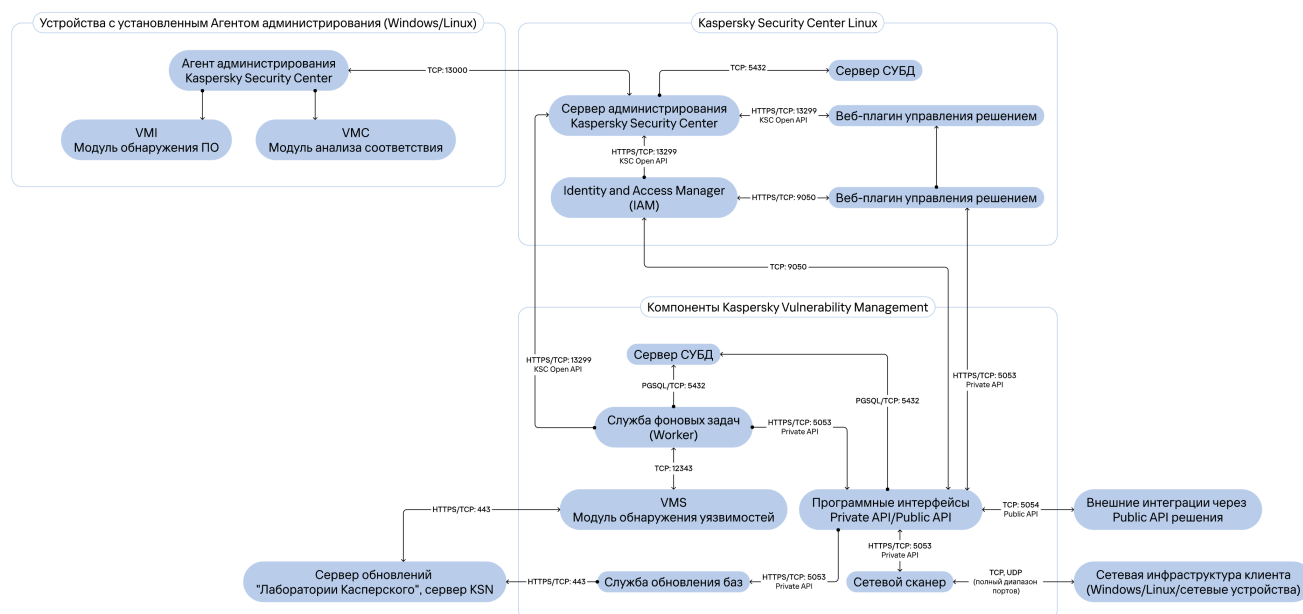
Kaspersky Vulnerability Management включает в себя следующие компоненты:

- **База данных.** Хранит данные решения.
- **Служба фоновых задач (Worker).** Выполняет служебные задачи и задачи, созданные для Kaspersky Vulnerability Management в Kaspersky Security Center.
- **Сетевой сканер.** Задействован в задачах *Безагентное сканирование в режиме белого ящика* и *Безагентное сканирование в режиме черного ящика*.
- **Private API.** Веб-служба для взаимодействия с веб-плагином управления решением через Kaspersky Security Center Web Console, Сетевым сканером и Службой фоновых задач.
- **Public API.** Веб-служба для взаимодействия внешних систем с Kaspersky Vulnerability Management.
- **VMS.** Модуль обнаружения уязвимостей. Задействован в задачах *Поиск уязвимостей* и *Безагентное сканирование в режиме белого ящика*.
- **VMI.** Модуль обнаружения программного обеспечения, установленного на устройствах. Выполняет инвентаризацию активов.
- **VMC.** Модуль анализа соответствия. Выполняет задачу *Сканирование активов на соответствие профилям*.
- **Служба обновления баз решения.** Веб-приложение, которое скачивает базы для Сетевого сканера, модулей VMD и VMC.

На рисунках ниже изображены схемы архитектуры решения в зависимости от варианта установки.



Компоненты Kaspersky Vulnerability Management и Сервера администрирования Kaspersky Security Center установлены на одном устройстве



Компоненты Kaspersky Vulnerability Management и Сервера администрирования Kaspersky Security Center установлены на разных устройствах

Комплект поставки

В комплект поставки Kaspersky Vulnerability Management входят следующие файлы:

kaspersky-vm-<номер версии>_amd64.deb	Пакет для установки решения в операционных системах, использующих формат пакетов <code>.deb</code> .
kaspersky-vm-<номер версии>-1.x86_64.rpm	Пакет для установки решения в операционных системах, использующих формат пакетов <code>.rpm</code> .
ksn.<идентификатор языка>	Файл с текстом Положения о KSN.
legal_notices.txt	Файл с информацией о стороннем коде.
license.<идентификатор языка>	Файл с текстом Лицензионного соглашения.
privacy.<идентификатор языка>	Файл с текстом Политики конфиденциальности.
webconsole-plugin.zip	ZIP-архив для установки веб-плагина управления Kaspersky Vulnerability Management через Kaspersky Security Center Web Console.
vm_integrity_manifest.xml	Файл манифеста для проверки целостности модулей Kaspersky Vulnerability Management.

Интерфейс решения

Управление решением осуществляется через интерфейс Kaspersky Security Center Web Console (далее также "Web Console") с помощью следующих элементов:

- Главное меню в левой части окна Web Console. Раздел главного меню, в котором расположены вложенные разделы для управления решением, называется **Управление уязвимостями**.
- Рабочая область в правой части окна Web Console. В рабочей области отображаются данные и элементы управления для выбранного раздела.

О входе в Kaspersky Security Center Web Console см. [в справке Kaspersky Security Center](#).

Данные во всех разделах решения представлены в виде таблиц.

В разделах Kaspersky Vulnerability Management в интерфейсе Web Console есть элементы, с помощью которых вы можете выполнять следующие действия:

- Обновлять данные в таблицах. С помощью кнопки **Обновить** в левом верхнем углу таблицы запустите обновление данных в таблице.
- Экспортировать данные в CSV-файл. В таблицах с уязвимостями и активами нажмите на кнопку **Экспортировать в CSV**.

Экспорт не работает при количестве записей более одного миллиона.

- Удалять данные из решения. В таблицах с помощью флажков слева от названий пользовательских профилей соответствия, шаблонов отчетов и сгенерированных отчетов выберите нужные и нажмите на кнопку **Удалить**.
- Выполнять поиск по данным в таблицах. В строке поиска над таблицей введите текст и нажмите на значок . Столбцы, по которым возможен поиск, указаны в строке поиска.
- Фильтровать данные в таблицах. Нажмите на значок  в правом верхнем углу таблицы, в открывшемся окне укажите и примените критерий для фильтрации данных в таблице.

- Отображать данные в таблицах. Нажмите на значок  в правом верхнем углу таблицы и в открывшемся окне выберите столбцы для отображения.
- Сортировать данные в таблицах. Нажмите на название столбца таблицы, в раскрывшемся меню выберите тип сортировки: по возрастанию или по убыванию. Справа от названия столбца, к которому применена сортировка, отображается значок, указывающий на тип сортировки.

Поддерживаемые операционные системы

Kaspersky Vulnerability Management поддерживает поиск уязвимостей в операционных системах, перечисленных ниже.

Операционные системы, поддерживаемые в базах данных уязвимостей для задачи Поиск уязвимостей.

- Альт Сервер 10
- Альт Сервер 11.0
- Альт СП Сервер 8.4
- Альт СП Сервер 10
- Альт СП Рабочая станция 10
- Альт Рабочая станция 11.2 ARM
- РЕД ОС 8.0
- Astra Linux Common Edition (очередное обновление 2.12)
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5) в режиме замкнутой программной среды
- Debian 11.0
- Debian 13.0
- Rocky Linux 9.6
- Ubuntu Server 22.04 LTS
- Ubuntu Server 24.04 LTS
- Ubuntu Server 26.04 LTS
- Windows 10 версии 1507, 1607, 1809, 21H2, 22H2
- Windows 11 25H2
- Windows Server 2025

Все перечисленные операционные системы 64-разрядные.

Операционные системы, поддерживаемые в базах данных уязвимостей для задачи Сканирование активов на соответствие профилям.

- РЕД ОС
- Семейство операционных систем Альт
- Astra Linux
- Debian
- Ubuntu
- Windows
- Windows Server

Поддерживаемое программное обеспечение

Kaspersky Vulnerability Management поддерживает поиск уязвимостей в программном обеспечении, перечисленном ниже.

Программное обеспечение, поддерживаемое в базе данных уязвимостей для задач Безагентное сканирование в режиме белого ящика и Поиск уязвимостей

Программное обеспечение, поддерживаемое в базе данных уязвимостей для задачи Безагентное сканирование в режиме черного ящика

Поддерживаемые профили соответствия

Kaspersky Vulnerability Management поддерживает сканирование активов на соответствие следующим профилям:

- Проверки конфигурации ОС Astra Linux на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС Astra Linux;
 - Профиль ФСТЭК России №21 для ОС Astra Linux;
 - Профиль ФСТЭК России №31 для ОС Astra Linux;
 - Профиль ФСТЭК России №239 для ОС Astra Linux;
 - Профиль Kaspersky C Basic для ОС Astra Linux;

- Профиль Kaspersky D Basic для ОС Astra Linux;
- Профиль KSC для ОС Astra Linux.
- Проверки конфигурации ОС Debian на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС Debian;
 - Профиль ФСТЭК России №21 для ОС Debian;
 - Профиль ФСТЭК России №31 для ОС Debian;
 - Профиль ФСТЭК России №239 для ОС Debian;
 - Профиль Kaspersky C Basic для ОС Debian;
 - Профиль Kaspersky D Basic для ОС Debian;
 - Профиль KSC для ОС Debian.
- Проверки конфигурации ОС Ubuntu на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС Ubuntu;
 - Профиль ФСТЭК России №21 для ОС Ubuntu;
 - Профиль ФСТЭК России №31 для ОС Ubuntu;
 - Профиль ФСТЭК России №239 для ОС Ubuntu;
 - Профиль Kaspersky C Basic для ОС Ubuntu;
 - Профиль Kaspersky D Basic для ОС Ubuntu;
 - Профиль KSC для ОС Ubuntu.
- Проверки конфигурации ОС ALT Linux на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС ALT Linux;
 - Профиль ФСТЭК России №21 для ОС ALT Linux;
 - Профиль ФСТЭК России №31 для ОС ALT Linux;
 - Профиль ФСТЭК России №239 для ОС ALT Linux;
 - Профиль Kaspersky C Basic для ОС ALT Linux;
 - Профиль Kaspersky D Basic для ОС ALT Linux;
 - Профиль KSC для ОС ALT Linux.

- Проверки конфигурации ОС RedOS на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС RedOS;
 - Профиль ФСТЭК России №21 для ОС RedOS;
 - Профиль ФСТЭК России №31 для ОС RedOS;
 - Профиль ФСТЭК России №239 для ОС RedOS;
 - Профиль Kaspersky C Basic для ОС RedOS;
 - Профиль Kaspersky D Basic для ОС RedOS;
 - Профиль KSC для ОС RedOS.
- Проверки конфигурации ОС Windows на соответствие требованиям нормативных, методических и организационных документов:
 - Профиль ФСТЭК России №117 для ОС Windows;
 - Профиль ФСТЭК России №21 для ОС Windows;
 - Профиль ФСТЭК России №31 для ОС Windows;
 - Профиль ФСТЭК России №239 для ОС Windows;
 - Профиль Kaspersky C Basic для ОС Windows;
 - Профиль Kaspersky D Basic для ОС Windows;
 - Профиль KSC для ОС Windows.

Профили D Basic составлены с учетом международных стандартов безопасности данных платежных систем.

Профили C Basic составлены с учетом международных рекомендаций и практик по кибербезопасности и защите ИТ-систем.

Профили KSC составлены с учетом Руководства по усилению защиты для Kaspersky Security Center.

Подготовка к работе

В этом разделе описаны шаги по подготовке необходимых компонентов и развертыванию Kaspersky Vulnerability Management.

Подготовка к развертыванию

Вы можете развернуть Kaspersky Vulnerability Management на одном устройстве с Сервером администрирования Kaspersky Security Center или на отдельном устройстве.

О поддерживаемых версиях приложений читайте в статье [Аппаратные и программные требования](#).

Перед развертыванием Kaspersky Vulnerability Management необходимо, чтобы были выполнены предварительные условия:

- На устройстве для развертывания Kaspersky Vulnerability Management или на отдельном устройстве:
 - [Установлен Сервер администрирования Kaspersky Security Center Linux](#).
 - На устройстве с установленным Сервером администрирования или отдельно [установлено приложение Kaspersky Security Center Web Console](#) с использованием Identity and Access Manager (IAM).
 - На устройстве с установленным Kaspersky Security Center Web Console [установлен веб-плагин для управления решением через Kaspersky Security Center Web Console](#).
 - На устройстве с установленным Kaspersky Security Center Web Console [созданы роли и учетные записи пользователей для решения](#).
- На устройстве для развертывания Kaspersky Vulnerability Management:
 - [Создана и настроена база данных решения в PostgreSQL](#) или Postgres Pro.
 - [Установлен Агент администрирования Kaspersky Security Center](#).
 - [Установлена утилита jq](#).
 - [Установлен OpenSSL для Linux](#).
 - [Установлена утилита curl для выполнения запросов к Kaspersky Security Center, а также базовые утилиты coreutils, bash, sed, grep, less, findutils](#).
 - [Загружен и применен ключ решения kaspersky_astra_pub_key.gpg](#), если развертывание Kaspersky Vulnerability Management планируется на устройстве под управлением операционной системы Astra Linux Special Edition в режиме замкнутой программной среды.
- На управляемых активах [установлен Агент администрирования Kaspersky Security Center](#).

Установка Сервера администрирования Kaspersky Security Center Linux

Сервер администрирования Kaspersky Security Center Linux как часть решения Kaspersky Vulnerability Management необходимо установить на устройстве для развертывания решения или на отдельном устройстве. Подробно об установке см. в [справке Kaspersky Security Center](#).

О поддерживаемых версиях Kaspersky Security Center Linux читайте в статье [Аппаратные и программные требования](#).

Установка Kaspersky Security Center Web Console

Kaspersky Security Center Web Console с использованием Identity and Access Manager (IAM) как часть решения Kaspersky Vulnerability Management необходимо установить на устройстве с установленным Сервером администрирования или на отдельном устройстве. Подробно об установке см. в [справке Kaspersky Security Center](#).

О поддерживаемых версиях Kaspersky Security Center Web Console читайте в статье [Аппаратные и программные требования](#).

Установка веб-плагина для управления решением

На устройстве с установленным Kaspersky Security Center Web Console необходимо установить веб-плагин для управления решением.

Чтобы установить веб-плагин для управления решением через Kaspersky Security Center Web Console:

1. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

Откроется список установленных веб-плагинов.

2. Нажмите на кнопку **Добавить из файла**.

3. В открывшемся окне загрузите архив с дистрибутивом веб-плагина vulnerability_management.zip и файл с подписью signature.txt. Эти файлы упакованы в архив webconsole-plugin.zip.

Архив webconsole-plugin.zip входит в [комплект поставки](#).

4. Нажмите на кнопку **Добавить**.

5. Дождитесь окончания установки и нажмите на кнопку **ОК** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов в разделе **Параметры** → **Веб-плагины**. В Web Console появится раздел **Управление уязвимостями**.

Создание учетных записей пользователей и настройка доступа по ролям

Перед развертыванием Kaspersky Vulnerability Management необходимо в Kaspersky Security Center Web Console создать базовые роли и учетные записи внутренних пользователей и назначить им созданные роли согласно таблице ниже.

Подробнее о создании роли см. в [справке Kaspersky Security Center](#).

Подробнее о создании учетной записи внутреннего пользователя см. в [справке Kaspersky Security Center](#).

Учетные записи пользователей для Kaspersky Vulnerability Management должны быть исключены из двухфакторной аутентификации. Подробнее см. в [справке Kaspersky Security Center](#).

Удаление базовых ролей и / или изменение прав, предоставленных ролям, приведет к ошибкам в работе решения.

Права, назначенные ролям Kaspersky Vulnerability Management, применимы ко всем устройствам.

Имя учетной записи	Роль, которую требуется назначить для учетной записи	Области, к которым требуется предоставить права для роли	Права, которые требуется предоставить для области
VM Admin	VM Admin – пользовательская роль для главного администратора Kaspersky Vulnerability Management.	Сервер администрирования Kaspersky Security Center: - Общие функции: - Базовая функциональность. - Управление системой: - Подключения. - Удаленное выполнение скриптов. - Инвентаризация оборудования. - Удаленная установка. - Инвентаризация приложений. - Системное администрирование.	- Чтение - Запись - Выполнение - Выполнение операций с выборками устройств
		Kaspersky Vulnerability Management: - Активы. - Группы активов. - Анализ соответствия. - Сетевое сканирование API.	- Чтение - Запись
		Kaspersky Vulnerability Management: - Публичный API: - Активы. - Программное обеспечение. - Уязвимости. - Программное обеспечение.	Чтение
		Kaspersky Vulnerability Management: Отчеты.	- Чтение - Запись - Выполнение
		Kaspersky Vulnerability Management: Уязвимости.	- Чтение - Выполнение
VM Worker	VM Worker – служебная роль для взаимодействия компонентов Worker, VM API, VMS и Сервер администрирования Kaspersky Security Center.	Сервер администрирования Kaspersky Security Center: - Общие функции: - Базовая функциональность.	- Чтение - Запись - Выполнение
		Сервер администрирования Kaspersky Security Center: - Управление системой: - Подключения. Kaspersky Vulnerability Management: - Уязвимости.	- Чтение - Выполнение
		Kaspersky Vulnerability Management: Анализ соответствия.	- Чтение - Запись
		Kaspersky Vulnerability Management:	Чтение

Имя учетной записи	Роль, которую требуется назначить для учетной записи	Области, к которым требуется предоставить права для роли	Права, которые требуется предоставить для области
		- Сетевое сканирование API. - Программное обеспечение.	
VM Scanner	VM Scanner – служебная роль для вызова API, специфичного для Сетевого сканера.	Сервер администрирования Kaspersky Security Center: - Общие функции: - Базовая функциональность.	Чтение
		Kaspersky Vulnerability Management: Сетевое сканирование API.	- Чтение - Запись

Создание и настройка базы данных решения в PostgreSQL

Чтобы создать и настроить базу данных Kaspersky Vulnerability Management в PostgreSQL:

1. С помощью любого доступного инструмента для работы с сервером баз данных PostgreSQL (например, psql) выполните команду для создания базы данных:

```
CREATE DATABASE "<Имя базы данных>" WITH OWNER=postgres ENCODING='UTF8' TABLESPACE=pg_default CONNECTION LIMIT=-1;
```

2. Создайте роль пользователя для Kaspersky Vulnerability Management:

```
CREATE ROLE "<Имя роли>" WITH PASSWORD '<Пароль>' LOGIN NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION;
```

3. Созданной роли пользователя предоставьте право на подключение к созданной базе данных:

```
GRANT CONNECT ON DATABASE "<Имя базы данных>" TO "<Имя роли>";
```

4. Перейдите в созданную базу данных:

```
\с "<Имя базы данных>";
```

5. Создайте схему с именем созданной роли пользователя в созданной базе данных:

```
CREATE SCHEMA "<Имя роли>" AUTHORIZATION "<Имя роли>";
```

6. Если необходимо, настройте защищенное TLS-соединение с созданной базой данных. Подробнее об этом см. в документации к PostgreSQL в статье [Защита соединений TCP/IP с применением SSL](#).

7. Для созданной роли пользователя настройте парольную аутентификацию в созданной базе данных:

Kaspersky Vulnerability Management не поддерживает аутентификацию другими способами (например, по сертификату или GSSAPI).

- a. Узнайте расположение конфигурационного файла pg_hba.conf:

```
psql -U postgres -d postgres -c "SHOW hba_file;"
```

- b. Откройте конфигурационный файл pg_hba.conf.

- c. Добавьте строку с настройками парольной аутентификации для созданной роли пользователя в созданной базе данных в следующем формате:

<тип подключения> "<Имя базы данных>" "<Имя роли>" <источник подключения> <метод аутентификации>.

В качестве источника подключения укажите IP-адрес устройства, на которое будут устанавливаться компоненты Kaspersky Vulnerability Management.

Подробнее о парольной аутентификации в базах данных PostgreSQL см. в документации к PostgreSQL в статье [Аутентификация password](#).

Подробнее о работе с конфигурационным файлом pg_hba.conf см. в документации к PostgreSQL в статье [Файл pg_hba.conf](#).

- d. Сохраните файл pg_hba.conf.

- e. Перезагрузите службу PostgreSQL:

```
systemctl reload postgresql;
```

Установка Агента администрирования Kaspersky Security Center

На устройстве для развертывания Kaspersky Vulnerability Management необходимо установить Агент администрирования [поддерживаемой версии](#).

На активах для сканирования необходимо установить Агент администрирования с поддержкой функциональности решения.

Подробнее об установке Агента администрирования см. в [справке Kaspersky Security Center](#). В процессе установки Агентов администрирования указывайте данные для подключения к Серверу администрирования, который используется [в составе решения](#).

О поддерживаемых версиях Агента администрирования и операционных системах, в которых Агент администрирования поддерживает функциональность решения, читайте в статье [Аппаратные и программные требования](#).

Установка утилиты jq

На устройстве для развертывания Kaspersky Vulnerability Management необходимо установить утилиту jq для парсинга JSON-данных. Для установки утилиты используйте менеджер пакетов, доступный в операционной системе.

Например, вы можете использовать одну из команд:

- `sudo apt install jq`
- `sudo yum install jq`

Установка OpenSSL для Linux

На устройстве для развертывания Kaspersky Vulnerability Management необходимо установить OpenSSL для Linux. Для установки утилиты используйте менеджер пакетов, доступный в операционной системе.

Например, вы можете использовать одну из команд:

- `sudo apt install openssl`
- `sudo yum install openssl`

Установка прочих необходимых утилит

На устройстве для развертывания Kaspersky Vulnerability Management необходимо установить утилиту curl для выполнения запросов к Kaspersky Security Center, а также проверить, что установлены утилиты операционной системы coreutils, bash, sed, grep, less, findutils. Для установки утилит используйте менеджер пакетов, доступный в операционной системе.

Например, вы можете использовать одну из команд:

- `sudo apt install <имя утилиты>`
- `sudo yum install <имя утилиты>`

Применение ключа решения kaspersky_astra_pub_key.gpg

Прежде чем разворачивать Kaspersky Vulnerability Management на устройстве под управлением операционной системы Astra Linux Special Edition в режиме замкнутой программной среды, требуется применить на устройстве ключ решения.

Чтобы применить на устройстве ключ решения:

1. Скачайте ключ решения [kaspersky_astra_pub_key.gpg](#).
2. В конфигурационном файле `/etc/digsig/digsig_initramfs.conf` укажите параметр `DIGSIG_ELF_MODE=1`.
3. Установите пакет совместимости:

```
apt install astra-digsig-oldkeys
```

4. Создайте директорию для ключа решения:

```
mkdir -p /etc/digsig/keys/legacy/kaspersky/
```

5. Поместите ключ решения в директорию, созданную на предыдущем шаге:

```
cp kaspersky_astra_pub_key.gpg /etc/digsig/keys/legacy/kaspersky/
```

6. Обновите исходный образ файловой системы RAM для всех ядер операционной системы:

```
update-initramfs -u -k all
```

7. Перезагрузите операционную систему.

Развертывание

Развертывание Kaspersky Vulnerability Management состоит из следующих этапов:

- 1 [Установка и настройка компонентов Kaspersky Vulnerability Management](#)
- 2 [Перезапуск службы Kaspersky Security Center Web Console Plugin](#)
- 3 [Включение решения на Сервере администрирования Kaspersky Security Center](#)
- 4 [Включение решения в Агентах администрирования на активах](#)

Установка и настройка компонентов Kaspersky Vulnerability Management

[Компоненты Kaspersky Vulnerability Management](#) обеспечивают основные функции решения.

Чтобы установить компоненты Kaspersky Vulnerability Management:

1. Откройте терминал.
2. С помощью команды `cd` перейдите в директорию, в которой хранится пакет для установки компонентов Kaspersky Vulnerability Management:
 - `kaspersky-vm_<номер версии>_amd64.deb` – для установки в операционных системах, использующих формат пакетов `.deb`;
 - `kaspersky-vm-<номер версии>-1.x86_64.rpm` – для установки в операционных системах, использующих формат пакетов `.rpm`.
3. Установите пакет с помощью одной из следующих команд:

- `sudo apt install ./kaspersky-vm_<номер версии>_amd64.deb` – в операционных системах, использующих формат пакетов `.deb`;
- `sudo yum localinstall ./kaspersky-vm-<номер версии>-1.x86_64.rpm` – в операционных системах, использующих формат пакетов `.rpm`;
- `sudo apt-get install ./kaspersky-vm-<номер версии>-1.x86_64.rpm` – в операционных системах семейства Альт.

По завершении установки будет выведено сообщение о том, как выполнить настройку Kaspersky Vulnerability Management.

4. Запустите помощника по настройке Kaspersky Vulnerability Management:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh configure
```

Запустится помощник по настройке Kaspersky Vulnerability Management. Выполните действия, которые он предложит.

5. Выберите язык, на котором будут отображаться интерфейс и системные сообщения решения: `ru` или `en`.
6. Ознакомьтесь с текстом Лицензионного соглашения.
7. Примите условия и положения Лицензионного соглашения, для этого введите `y`.
8. Ознакомьтесь с текстом Политики конфиденциальности.
9. Примите условия Политики конфиденциальности, для этого введите `y`.
10. Ознакомьтесь с текстом Положения о KSN.
11. Укажите решение насчет согласия с условиями Положения о KSN, для этого введите `y` или `n`.

Функциональность KSN может быть недоступна в решении на территории США.

12. Введите данные для подключения к [предварительно созданной базе данных решения](#):
- a. FQDN или IP-адрес устройства с созданной базой данных.
 - b. Номер порта для подключения к устройству с созданной базой данных. По умолчанию – 5432.
 - c. Имя базы данных.
 - d. Имя и пароль роли пользователя для решения в базе данных.
 - e. Выберите режим SSL для подключения к базе данных: `disable`, `allow`, `prefer`, `require`, `verify-ca`, `verify-full`. Подробнее о каждом режиме см. в [документации к PostgreSQL](#).
 - f. Если на предыдущем шаге выбран режим `require`, `verify-ca` или `verify-full`, укажите путь к SSL-сертификату базы данных.
13. Для доступа к [обновляемым базам](#) введите значения параметров прокси-сервера:
- a. Включено ли использование прокси-сервера: `true` или `false`.
 - b. Если на предыдущем шаге введено значение `true`, для подключения к прокси-серверу введите адрес прокси-сервера в формате `proxy.example.com`, порт прокси-сервера (по умолчанию – 8080), имя пользователя и пароль для аутентификации на прокси-сервере. Значения этих параметров вы можете посмотреть в Kaspersky Security Center Web Console в разделе **Параметры** → **Интеграция** на вкладке **Параметры прокси-сервера Web Console**.
14. Введите адрес для доступа к Kaspersky Security Center API в формате `https://ksc.example.com:13299`.
15. Введите адрес для доступа к Kaspersky Security Center IAM Proxy в формате `https://ksc-iam.example.com:9050`.
16. В строке с предложением автоматически создать TLS-сертификаты для служб Kaspersky Vulnerability Management введите `y` или `n`.
17. Если на предыдущем шаге вы ввели `n`, введите необходимые данные о TLS-сертификатах и приватных ключах для служб Kaspersky Vulnerability Management:

TLS-сертификаты для служб должны быть выписаны специально для Kaspersky Vulnerability Management. Приватные ключи должны быть незашифрованными.

- a. Укажите тип используемых сертификатов:
 - `1` – сертификаты от центра сертификации;
 - `2` – самоподписанные сертификаты.
- b. Введите пути к TLS-сертификату и приватному ключу для службы Private API.
- c. Введите пути к TLS-сертификату и приватному ключу для службы Public API.
- d. Введите пути к TLS-сертификату и приватному ключу для службы VMS.

Если срок действия какого-либо из сертификатов истекает, решение перестает функционировать. Для избежания такой ситуации рекомендуем раз в год делать ротацию сертификатов с помощью параметра `rotate-certs` [помощника по настройке](#).

18. Введите имя учетной записи VM Scanner с ролью VM Scanner, [созданной перед установкой компонентов Kaspersky Vulnerability Management](#).
19. Введите пароль учетной записи VM Scanner.
20. Введите имя учетной записи VM Worker, [созданной перед установкой компонентов Kaspersky Vulnerability Management](#).
21. Введите пароль учетной записи VM Worker.

Помощник по настройке выполнит необходимые проверки и установит компоненты Kaspersky Vulnerability Management.

Если какие-то проверки пройдут неуспешно, например, связность с Kaspersky Security Center API будет отсутствовать или учетные данные пользователей окажутся неверными, помощник по настройке предложит ввести данные вновь.

Вы также можете запускать настройку параметров Kaspersky Vulnerability Management в неинтерактивном режиме с помощью команды:

```
sudo KVMANSWERSFILE=/path/to/file.json /opt/kaspersky/vulnerability-management/helper/helper.sh  
unattendedconfigure
```

Где `/path/to/file.json` – путь к JSON-файлу с параметрами для настройки Kaspersky Vulnerability Management.

```
{  
  "eulaAccepted":true,  
  "privacyPolicyAccepted":true,  
  "ksnAgreementAccepted":true|false,  
  "database":  
  {  
    "host": "",  
    "port": ,  
    "dbname": "",  
    "dbschema": "",  
    "dbuser": "",  
    "dbpassword": "",  
    "dbssl":  
    {  
      "mode": "verify-full|disable|allow|prefer|require|verify-ca",  
      "certpath": ""  
    }  
  },  
  "proxy":  
  {  
    "enabled":true|false,  
    "host": "",  
    "port": ,  
    "login": "",  
    "password": ""  
  },  
  "ksc":  
  {  
    "apiurl": "",  
    "iamproxyurl": "",  
    "users":  
  }  
}
```

```

{
  "worker":
  {
    "username": "",
    "password": ""
  },
  "scanner":
  {
    "username": "",
    "password": ""
  }
},
"tls":
{
  "certificates": "generate|existing",
  "existing":
  {
    "type": "ca|selfsigned",
    "services":
    {
      "ca":
      {
        "certpath": ""
      },
      "privateapi":
      {
        "certpath": "",
        "keypath": ""
      },
      "publicapi":
      {
        "certpath": "",
        "keypath": ""
      },
      "vms":
      {
        "certpath": "",
        "keypath": ""
      }
    }
  }
}
}

```

Параметры файла `file.json` определяют следующее:

`.eulaAccepted` (boolean) — признак согласия с Лицензионным соглашением. Для продолжения настройки должен быть `true`.

`.privacyPolicyAccepted` (boolean) — признак согласия с "Политикой конфиденциальности". Для продолжения настройки должен быть `true`.

`.ksnAgreementAccepted` (boolean) — признак принятия Положения о KSN, влияет на работу модуля обнаружения уязвимостей. Возможные значения: `true` или `false`.

Функциональность KSN может быть недоступна в решении на территории США.

`.database.host` (string) — FQDN или IP-адрес для доступа к устройству с созданной базой данных решения.

`.database.port` (int) — номер порта для доступа к устройству с созданной базой данных решения.

`.database.dbname` (string) — имя базы данных решения.

`.database.dbschema` (string) — схема в базе данных, с которой будет работать решение.

`.database.dbuser` (string) — имя роли пользователя для решения в базе данных.

`.database.dbpassword` (string) — пароль роли пользователя для решения в базе данных.

`.database.dbssl.mode` (string) — режим SSL для подключения к базе данных. Возможные значения: `verify-full|disable|allow|prefer|require|verify-ca`. Подробнее о каждом режиме см. в [документации к PostgreSQL](#).

`.database.dbssl.certpath` (string) — путь к SSL-сертификату базы данных. Обязателен, если для параметра `.database.dbssl.mode` указано одно из значений `verify-full|require|verify-ca`.

`.proxy.enabled` (boolean) — признак, определяющий необходимость использовать прокси-сервер для доступа к [обновляемым базам](#). Если значение равно `true`, то все остальные значения раздела `.proxy` должны быть указаны. Значения этих параметров вы можете посмотреть в Kaspersky Security Center Web Console в разделе **Параметры** → **Интеграция** на вкладке **Параметры прокси-сервера Web Console**.

`.proxy.host` (string) — адрес прокси-сервера в формате `proxy.example.com`.

`.proxy.port` (int) — порт прокси-сервера (по умолчанию — 8080).

`.proxy.login` (string) — имя пользователя для аутентификации на прокси-сервере. Для анонимной аутентификации на прокси-сервере не указывайте значение.

`.proxy.password` (string) — пароль пользователя для аутентификации на прокси-сервере. Для анонимной аутентификации на прокси-сервере не указывайте значение.

`.ksc.apiurl` (string) — адрес для доступа к Kaspersky Security Center API в формате `https://ksc.example.com:13299`.

`.ksc.iamproxyurl` (string) — адрес для доступа к Kaspersky Security Center IAM Proxy в формате `https://ksc-iam.example.com:9050`.

`.ksc.users.worker.username` (string) — имя учетной записи VM Worker, [созданной перед установкой компонентов Kaspersky Vulnerability Management](#).

`.ksc.users.worker.password` (string) — пароль учетной записи VM Worker.

`.ksc.users.scanner.username` (string) — имя учетной записи VM Scanner с ролью VM Scanner, созданной перед установкой компонентов Kaspersky Vulnerability Management.

`.ksc.users.scanner.password` (string) — пароль учетной записи VM Scanner.

`.tls.certificates` (string) — способ указания TLS-сертификатов. Возможные значения:

- `generate`. Если указано это значение, помощник по настройке самостоятельно создает TLS-сертификаты, заполнять остальные поля в блоке `.tls` не требуется.
- `existing`. Если указано это значение, необходимо ввести пути к заранее созданным TLS-сертификатам и заполнить остальные поля в блоке `.tls`.

`.tls.existing.type` (string) — тип заранее созданных TLS-сертификатов. Возможные значения:

- `ca`. Сертификаты выписаны корпоративным центром сертификации. Все сертификаты должны быть выписаны одними и теми же корневым и промежуточным (если такой используется в организации) центрами сертификации.
- `selfsigned`. Самоподписанные сертификаты.

`.tls.existing.services.ca.certpath` (string) — путь к файлу с цепочкой сертификатов корпоративного центра сертификации. Должен содержать сертификаты как корневого, так и промежуточного (если используется в организации) центров сертификации. Поле не требуется заполнять, если `.tls.existing.type` имеет значение `selfsigned`.

`.tls.existing.services.privateapi.certpath` (string) — путь к файлу с сертификатом для Private API. Файл должен быть незашифрованным.

`.tls.existing.services.privateapi.keypath` (string) — путь к файлу с ключом сертификата для Private API. Файл должен быть незашифрованным.

`.tls.existing.services.publicapi.certpath` (string) — путь к файлу с сертификатом для Public API. Файл должен быть незашифрованным.

`.tls.existing.services.publicapi.keypath` (string) — путь к файлу с ключом сертификата для Public API. Файл должен быть незашифрованным.

`.tls.existing.services.vms.certpath` (string) — путь к файлу с сертификатом для VMS. Файл должен быть незашифрованным.

`.tls.existing.services.vms.keypath` (string) — Путь к файлу с ключом сертификата для VMS. Файл должен быть незашифрованным.

Сразу после установки компонентов решения базы уязвимостей могут быть устаревшими. Для их автоматического обновления необходим доступ в интернет. Если доступа в интернет нет, вы можете [обновить базы уязвимостей с помощью Kaspersky Update Utility](#).

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`.

Если в процессе установки или настройки решения возникают какие-либо проблемы, вы можете [использовать помощника по настройке](#).

Перезапуск службы Kaspersky Security Center Web Console Plugin

Чтобы в веб-плагине управления решением после установки компонентов Kaspersky Vulnerability Management обновились данные, необходимо перезапустить службу Kaspersky Security Center Web Console Plugin.

Чтобы перезапустить службу Kaspersky Security Center Web Console Plugin, выполните следующую команду:

```
systemctl restart KSCWebConsolePlugin.service
```

Включение решения на Сервере администрирования

Чтобы включить Kaspersky Vulnerability Management на Сервере администрирования Kaspersky Security Center:

1. На устройстве с установленным Сервером администрирования выполните следующую команду:

```
/opt/kaspersky/ksc64/sbin/klscflag -fset -pv ".core/.independent" -s klcsff -n KLCS_FF_VMGMT_SUPPORT -t d -v 1
```

2. Перезапустите службу Сервера администрирования с помощью следующей команды:

```
systemctl restart kladminserver_srv.service
```

Включение решения в Агентах администрирования активов

Агент администрирования Kaspersky Security Center участвует в [инвентаризации активов](#) и [сканировании активов на соответствие профилям](#). Необходимая функциональность Kaspersky Vulnerability Management поддерживается, но выключена по умолчанию в Агентах администрирования.

Чтобы включить Kaspersky Vulnerability Management в Агентах администрирования:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Создайте новую или откройте существующую политику с настройками для Агента администрирования Kaspersky Security Center. Подробнее о создании и настройке политик см. в [справке Kaspersky Security Center Linux](#).
3. Откройте вкладку **Параметры приложения** политики.
4. В разделе **Обновления и уязвимости в приложениях** переведите переключатель **Включить Kaspersky Vulnerability Management** в активное положение.
5. Нажмите на кнопку **Сохранить**.
6. Установите [блокировку \(замок\)](#) для измененной политики и дождитесь ее применения.

После применения созданной или измененной политики функциональность Kaspersky Vulnerability Management будет включена в Агентах администрирования, установленных на устройствах, входящих в группу Kaspersky Security Center **Управляемые устройства**.

Работа с активами

Актив – это рабочая станция или сервер в ИТ-инфраструктуре организации. Решение выполняет поиск и управление уязвимостями на активах.

В этом разделе описан механизм получения данных об активах и действия, которые вы можете выполнять с активами.

Инвентаризация активов

Инвентаризация активов – процесс получения данных об активах.

Kaspersky Vulnerability Management каждые 60 минут обращается к Серверу администрирования Kaspersky Security Center для импорта данных обо всех управляемых и нераспределенных активах, зарегистрированных в Kaspersky Security Center.

Данные об активах обогащаются в результате [инвентаризации программного обеспечения](#), которая предоставляет данные об установленных приложениях, и выполнения [сканирования](#), результаты которого поставляют данные об обнаруженных уязвимостях, найденных открытых портах и службах, соответствии профилям.

Данные об активах отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Активы** отображается список активов, зарегистрированных в Kaspersky Vulnerability Management. По ссылке на имени актива открывается карточка актива, содержащая следующую информацию об активе:
 - **Основная информация.** Значимость актива, которая по умолчанию не определена, описание и другая сопутствующая информация; сетевые и системные параметры.
 - **Обнаруженные уязвимости.** Данные об уязвимостях, обнаруженных на активе.
 - **Установленное ПО.** Список приложений, установленных на активе.
 - **Сетевое сканирование.** Результаты [сетевого сканирования](#) на наличие открытых портов и служб, доступных через открытые порты.
 - **Анализ соответствия.** Результаты [сканирования активов на соответствие профилям](#).
- В разделе **Управление уязвимостями** → **Уязвимости** в таблице и в карточках уязвимостей отображаются активы, на которых обнаружены уязвимости.
- В разделе **Управление уязвимостями** → **Программное обеспечение** в карточке приложения на вкладке **Установлено на активах** отображается список активов, на которых установлено приложение.

Активы, которые уже удалены с Сервера администрирования, удаляются из базы данных решения в течение 30 минут после очередного импорта данных обо всех управляемых и нераспределенных активах, зарегистрированных в Kaspersky Security Center.

Информация об удалении активов из базы данных Kaspersky Vulnerability Management не сохраняется.

Изменение значимости активов

Определение значимости активов необходимо для приоритизации активов. Например, в организации есть активы, которые принадлежат нетехническим специалистам с минимальным набором прав и задач. Такие активы неприоритетны с точки зрения потенциальной уязвимости и влияния на ИТ-инфраструктуру. Значимость таких активов можно считать низкой.

Значимость активов участвует в расчете приоритета устранения уязвимостей по [методике ФСТЭК](#).

По умолчанию, значимость активов не определена. Вы можете указывать и изменять значимость активов.

Как указать или изменить значимость активов в таблице активов

1. В главном окне Web Console выберите **Управление уязвимостями** → **Активы**.
2. С помощью флажков слева от имен активов выберите один или несколько активов, значимость которых вы хотите указать или изменить.
3. Нажмите на кнопку **Изменить значимость**.
Откроется окно **Изменить значимость**.
4. В списке значений выберите значимость:
 - Критичная.
 - Высокая.
 - Средняя.
 - Низкая.
 - Не определена.
5. Нажмите на кнопку **Сохранить**.

В таблице активов в столбце **Значимость** напротив имен активов отобразится новое значение значимости актива.

Как указать или изменить значимость актива в карточке актива

1. В главном окне Web Console выберите **Управление уязвимостями** → **Активы**.
2. Перейдите по ссылке на имени актива, значимость которого вы хотите указать или изменить.
Откроется карточка актива.
3. На вкладке **Основная информация** в раскрывающемся списке **Значимость** выберите нужное значение:
 - Критичная.
 - Высокая.
 - Средняя.

- Низкая.
- Не определена.

4. Нажмите на кнопку **Сохранить**.

В таблице активов в столбце **Значимость** напротив имени актива отобразится новое значение значимости актива.

Работа с группами активов

Вы можете объединять активы в группы для удобства настройки [задач Kaspersky Vulnerability Management](#) – на шаге выбора активов для сканирования доступен выбор групп активов.

Kaspersky Vulnerability Management добавляет активы в группу автоматически, если они удовлетворяют условиям включения в группу активов. Таким образом, новые активы динамически учитываются в группе активов.

Вы можете добавлять, изменять и удалять группы активов.

Как добавить группу активов

1. В главном окне Web Console выберите **Управление уязвимостями → Группы активов**.
2. Нажмите на кнопку **Добавить**.
Откроется окно **Добавление группы активов**.
3. Введите название группы в одноименном поле.
4. Выберите оператор между условиями включения в группу активов:
 - **И**. При добавлении нескольких условий между ними применяется логическое И. Выбрано по умолчанию.
 - **ИЛИ**. При добавлении нескольких условий между ними применяется логическое ИЛИ.
5. Сформируйте одно или несколько условия включения в группу активов:
 - а. Для каждого условия выберите параметр актива и оператор, далее введите значение параметра.
 - б. Используйте кнопку **Добавить условие** для добавления каждого следующего условия.
6. Нажмите на кнопку **Проверить условия** чтобы получить список активов, которые удовлетворяют условиям.
7. Если необходимо, скорректируйте условия включения в группу активов. Вы можете удалить все условия с помощью кнопки **Очистить все**.
8. Нажмите на кнопку **Сохранить**.

Группа активов отобразится в таблице **Группы активов**.

Как изменить группу активов

1. В главном окне Web Console выберите **Управление уязвимостями** → **Группы активов**.
2. Нажмите на ссылку на названии группы активов, которую вы хотите удалить.
Откроется окно с параметрами группы активов.
3. Если необходимо, измените название группы в одноименном поле.
4. Если необходимо, измените оператор между условиями включения в группу активов:
 - **И**. При добавлении нескольких условий между ними применяется логическое И.
 - **ИЛИ**. При добавлении нескольких условий между ними применяется логическое ИЛИ.
5. Если необходимо, измените условия включения в группу активов:
 - Вы можете удалить все условия с помощью кнопки **Очистить все**.
 - Для каждого условия выберите параметр актива и оператор, далее введите значение параметра.
 - Используйте кнопку **Добавить условие** для добавления каждого следующего условия.
6. Нажмите на кнопку **Проверить условия** чтобы получить список активов, которые удовлетворяют условиям.
7. Если необходимо, скорректируйте условия включения в группу активов.
8. Нажмите на кнопку **Сохранить**.

Как удалить группы активов

1. В главном окне Web Console выберите **Управление уязвимостями** → **Группы активов**.
2. С помощью флажков около названий групп активов выберите одну или несколько групп, которые вы хотите удалить.
3. Нажмите на кнопку **Удалить**.

Группы активов будут удалены.

Если на момент выполнения [задачи Kaspersky Vulnerability Management](#) удалены все группы активов, указанные в области действия задачи, то выполнение такой задачи завершается с ошибкой.

Если на момент выполнения задачи Kaspersky Vulnerability Management удалена часть групп активов, указанных в области действия задачи, то задача выполняется только для существующих групп активов.

Инвентаризация программного обеспечения

Инвентаризация программного обеспечения – процесс получения данных о программном обеспечении, которое установлено на активах, зарегистрированных в базе данных Kaspersky Vulnerability Management.

Kaspersky Vulnerability Management с помощью модуля обнаружения программного обеспечения (VMI) получает данные об установленных на активах приложениях из следующих источников:

- Сервер администрирования. Для получения данных о программном обеспечении, установленном на активах, необходимо, чтобы в Агентах администрирования Kaspersky Security Center, установленных на активах, была [включена функциональность Kaspersky Vulnerability Management](#).
- Результаты [безагентного сканирования активов в режиме белого ящика](#).

Данные о программном обеспечении отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Программное обеспечение** отображается список приложений, установленных на активах, которые зарегистрированы в Kaspersky Vulnerability Management. При переходе по ссылке в названии приложения открывается карточка приложения, которая содержит описание приложения, информацию о найденных в приложении уязвимостях и об активах, на которых установлено приложение.
- В разделе **Управление уязвимостями** → **Уязвимости** в таблице и в карточках уязвимостей отображаются приложения, в которых обнаружены уязвимости.
- В разделе **Управление уязвимостями** → **Активы** в карточках устройств на вкладке **Установленное ПО** отображаются приложения, установленные на активах.

Kaspersky Vulnerability Management получает данные о следующем **программном обеспечении**.

Kaspersky Vulnerability Management поддерживает инвентаризацию перечисленного выше программного обеспечения, установленного на активах, которые управляются следующими **операционными системами**.

- Альт Сервер 10
- Альт Сервер 11.0
- Альт СП Сервер 8.4
- Альт СП Сервер 10
- Альт СП Рабочая станция 10
- Альт Рабочая станция 11.2 ARM
- РЕД ОС 8.0
- Astra Linux Common Edition (очередное обновление 2.12)
- Astra Linux Special Edition РУСБ.10015-01 (очередное обновление 1.8.5) в режиме замкнутой программной среды
- Debian 11.0
- Debian 13.0
- Rocky Linux 9.6
- Ubuntu Server 22.04 LTS

- Ubuntu Server 24.04 LTS
- Ubuntu Server 26.04 LTS
- Windows 10 версии 1507, 1607, 1809, 21H2, 22H2
- Windows 11 25H2
- Windows Server 2025

Все перечисленные операционные системы 64-разрядные.

Настройка и выполнение сканирования

В этом разделе описаны настройка, запуск и результаты выполнения задач сканирования.

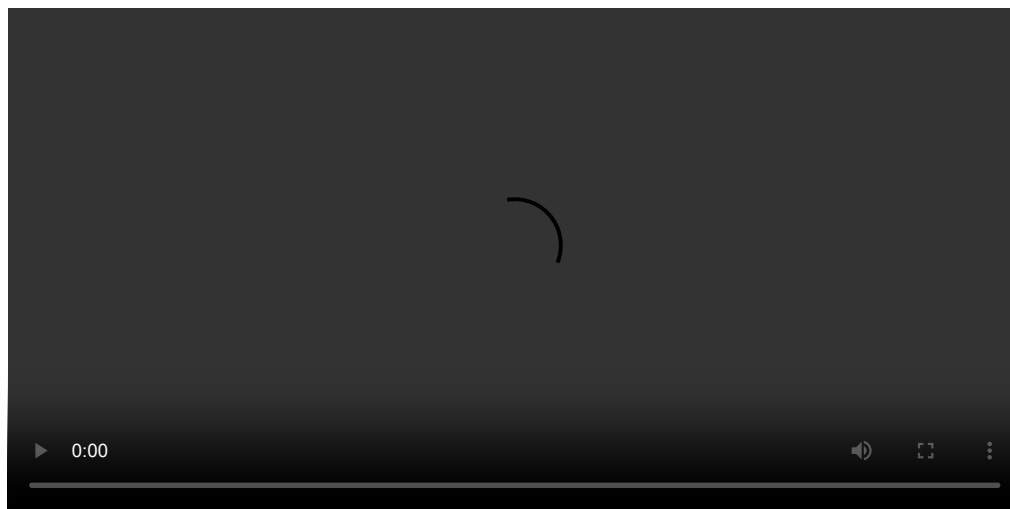
О типах сканирования

Для сканирования активов на уязвимости и для анализа соответствия активов стандартам предусмотрены следующие задачи Kaspersky Vulnerability Management:

- [Безагентное сканирование в режиме белого ящика](#). С помощью этой задачи Kaspersky Vulnerability Management выполняет сбор данных о программном обеспечении, установленном на активах, и поиск уязвимостей в нем. Для выполнения задачи требуется настройка доступа к данным активов внутри их операционных систем с помощью учетной записи и не требуется установка на активах сканирующего агента.
- [Безагентное сканирование в режиме черного ящика](#). С помощью этой задачи Kaspersky Vulnerability Management выполняет поиск открытых портов, служб, доступных через открытые порты, и уязвимостей служб. Для выполнения задачи не требуется установка на активах сканирующего агента и использование на активах данных учетных записей.
- [Поиск уязвимостей](#). С помощью этой задачи Kaspersky Vulnerability Management выполняет поиск уязвимостей в зарегистрированном в базе данных решения программном обеспечении.
- [Сканирование активов на соответствие профилям](#). С помощью этой задачи Kaspersky Vulnerability Management проверяет активы на соответствие внутренним, отраслевым и регуляторным требованиям безопасности.

Создание и настройка задач сканирования

Для наглядного ознакомления с настройкой общих параметров задач сканирования вы можете просмотреть видео ниже.



Чтобы создать и настроить задачу сканирования:

1. В главном окне Web Console выберите **Задачи**.

2. Нажмите на кнопку **Добавить**.

Откроется Мастер создания задачи. Для перехода к следующему шагу используйте кнопку **Далее**.

3. В раскрывающемся списке **Приложение** выберите **Kaspersky Vulnerability Management**.

4. В раскрывающемся списке **Тип задачи** выберите одну из задач:

- *Безагентное сканирование в режиме белого ящика.*
- *Безагентное сканирование в режиме черного ящика.*
- *Поиск уязвимостей.*
- *Сканирование активов на соответствие профилям.*

5. Укажите название задачи, которую вы создаете. Название задачи не может превышать 100 символов и не может содержать специальные символы: "*<>?\|;".

6. В блоке **Устройства, которым будет назначена задача** выберите вариант, который включает или позволяет указать устройство, на котором установлены компоненты Kaspersky Vulnerability Management.

7. На шаге **Область действия задачи** выберите устройство, на котором установлены компоненты Kaspersky Vulnerability Management.

8. На шаге **Активы для сканирования** укажите активы, на которых решение будет искать уязвимости или выполнять анализ соответствия стандартам. В зависимости от задачи доступны следующие варианты:

- **Выбранные активы.** Поиск уязвимостей или анализ соответствия стандартам будет выполняться на активах, добавленных в список с помощью кнопки **Добавить активы**.

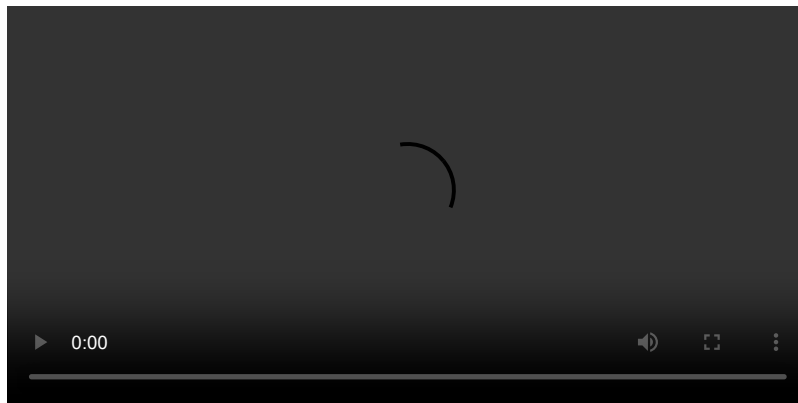
Если вы указываете IP-диапазон, включающий хотя бы одно устройство, не зарегистрированное в базе данных Kaspersky Security Center (например, на нем не установлен Агент администрирования), создание задачи завершится с ошибкой.

- **Группы активов.** Поиск уязвимостей или анализ соответствия стандартам будет выполняться на активах, входящих в [группы активов](#), добавленные в список с помощью кнопки **Добавить группы**.
- **Все активы.** Поиск уязвимостей будет выполняться на всех активах, зарегистрированных в базе данных решения в момент запуска задачи.

9. В зависимости от создаваемой задачи настройте следующие параметры:

- **Для задачи Безагентное сканирование в режиме белого ящика**

Для наглядного ознакомления с настройкой параметров задачи *Безагентное сканирование в режиме белого ящика* вы можете просмотреть видео ниже.



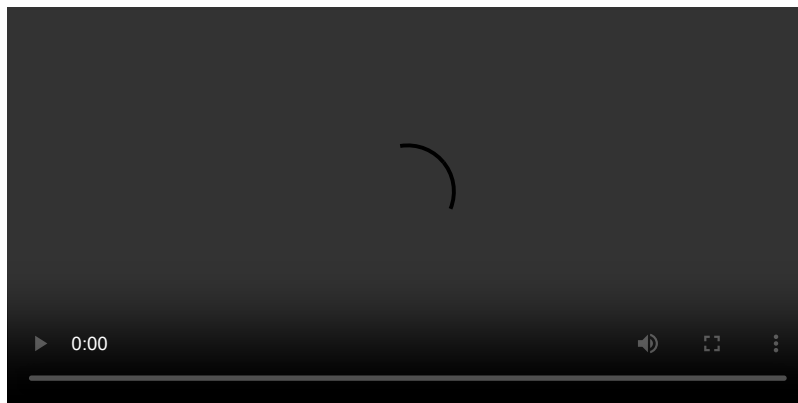
- На шаге **Настройки подключения по SSH** в поле **Имя пользователя** введите имя учетной записи пользователя, под которой Сетевой сканер будет подключаться к активам, выбранным для сканирования на шаге **Активы для сканирования**.
- В поле **Порт SSH** введите номер порта для подключения по протоколу SSH к активам для сканирования. По умолчанию введено значение 22.
- С помощью кнопки **Скачать** скачайте публичный ключ.
- На активах для сканирования создайте учетную запись пользователя с именем, указанным в пункте 9а. Например, с помощью команды `adduser` или `useradd`.
Учетная запись пользователя должна иметь права на операции `rpm` или `dpkg`.
В настройках SSH-сервера на активах должна быть включена аутентификация с помощью публичного ключа: в конфигурационном файле `sshd_config` в директории `/etc/ssh/` или `/etc/ssh/sshd_config.d` должна быть строка `PubkeyAuthentication yes`. Если вы изменили конфигурационный файл, необходимо перезапустить службу SSH для применения настроек. Например, с помощью команды `sudo systemctl restart ssh`.
- На активах для сканирования поместите публичный ключ, скачанный на шаге 9с инструкции, в домашней директории созданной учетной записи пользователя (например, `/home/<user name>/.ssh/authorized_keys`).
- На шаге **Дополнительные настройки**, если необходимо, измените значение параметра **Количество попыток подключения** – Сетевой сканер пробует подключиться к активу для сканирования указанное количество раз. Возможные значения – от 1 до 20. Значение по умолчанию равно одной попытке.
- Если необходимо, измените значение параметра **Интервал между попытками (сек.)** – в течение этого периода после неудачной попытки подключения к активу Сетевой сканер ожидает до следующей попытки подключиться к активу для сканирования. Возможные значения – от 1 до 100000. Значение по умолчанию равно одной секунде.

- h. Если необходимо, измените значение параметра **Максимум одновременных запросов** – Сетевой сканер одновременно выполняет указанное количество SSH-запросов к активам по указанному в пункте 9b инструкции номеру порта. Возможные значения – от 1 до 100000. По умолчанию указано значение 10000.

Параметр влияет на производительность решения. Для сохранения работоспособности решения рекомендуем ориентироваться на аппаратные характеристики устройства, на котором установлены компоненты Kaspersky Vulnerability Management.

- **Для задачи Безагентное сканирование в режиме черного ящика**

Для наглядного ознакомления с настройкой параметров задачи *Безагентное сканирование в режиме черного ящика* вы можете просмотреть видео ниже.



- a. В блоке **TCP-порты** в поле **Сканировать**, если необходимо, введите номера TCP-портов, которые будет сканировать Сетевой сканер. Для удобства ввода вы можете использовать ссылки **Все порты** и **Наиболее уязвимые порты**.

Вы можете вводить порты следующими способами:

- Отдельные номера портов в диапазоне от 0 до 65535, разделенные запятой.
- Диапазон портов в виде двух чисел от 0 до 65535, разделенных дефисом. Номер начального порта должен быть меньше или равен номеру конечного порта.
- Произвольная комбинация предыдущих вариантов, разделенных запятыми.

В некоторых шаблонах поиска уязвимостей прописаны порты для сканирования, которые могут не совпадать со списком портов, заданных при создании задачи. Такие порты и службы, доступные через эти порты, могут отобразиться в свойствах актива на вкладке **Сетевое сканирование**. Данное поведение не является ошибкой.

Поле обязательно для заполнения, если в блоке **UDP-порты** в поле **Сканировать** не введен хотя бы один номер.

- b. В поле **Исключить**, если необходимо, введите номера TCP-портов, которые будут исключены из сканирования.
- c. В блоке **UDP-порты** в поле **Сканировать**, если необходимо, введите номера UDP-портов, которые будет сканировать Сетевой сканер. Для удобства ввода вы можете использовать ссылки **Все порты** и **Наиболее уязвимые порты**.

Поле обязательно для заполнения, если в блоке **TCP-порты** в поле **Сканировать** не введен хотя бы один номер.

- d. В поле **Исключить**, если необходимо, введите номера UDP-портов, которые будут исключены из сканирования.
- e. С помощью переключателя **Сканировать сервисы** выключите или включите поиск служб, доступных через обнаруженные на активах открытые порты.
- f. С помощью переключателя **Сканировать на уязвимости** выключите или включите поиск уязвимостей в службах, доступных через обнаруженные на активах открытые порты.
- g. Выберите область поиска уязвимостей: **Все уязвимости** или **Выбранные уязвимости**.
- h. В зависимости от выбранной области поиска уязвимостей, в раскрывающемся списке **Исключить / Уязвимости** выберите один или несколько идентификаторов уязвимости для исключения или включения в сканирование, соответственно.
- i. Нажмите на кнопку **Далее**.
- j. В окне **Дополнительные параметры**, если необходимо, измените значение параметра **Время ожидания подключения (сек.)** – в течение этого периода после неудачной попытки подключения к активу Сетевой сканер ожидает до следующей попытки подключиться к активу для сканирования. Возможные значения – от 1 до 100000. Значение по умолчанию равно одной секунде.
- k. Если необходимо, измените значение параметра **Повторы при ошибке** – Сетевой сканер пробует подключиться к активу для сканирования указанное количество раз. Возможные значения – от 1 до 20. Значение по умолчанию равно одной попытке.
- l. Если необходимо, измените значение параметра **Максимум одновременных запросов** – Сетевой сканер одновременно выполняет указанное количество TCP / UDP-запросов к активам по указанным в задаче номерам портов. Возможные значения – от 1 до 100000. По умолчанию указано значение 10000.

В [конфигурационном файле](#) `scanner.json` вы можете также изменять значение параметра `scan.workerpool.count`, который определяет допустимое количество параллельно выполняющихся задач *Безагентное сканирование в режиме черного ящика*. При изменении значений параметров рекомендуем придерживаться следующих конфигураций:

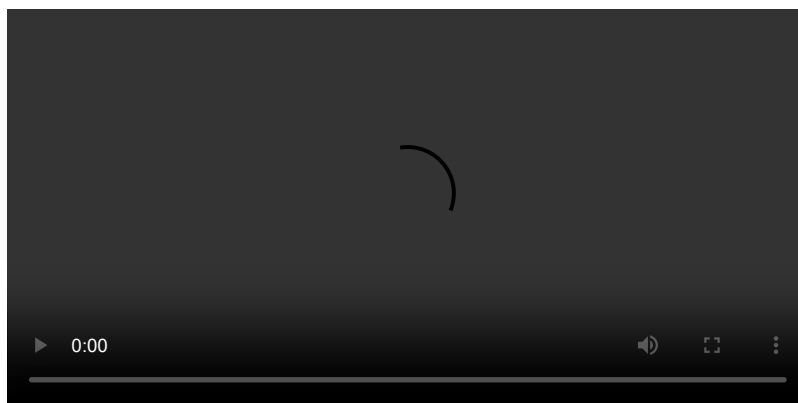
- *Безопасная*. Предполагает значения параметров **Максимум одновременных запросов** и `scan.workerpool.count` равными 10000 и 5, соответственно. Такая конфигурация требует около 4 ГБ оперативной памяти и загружает процессор на 10-20%.
- *Базовая*. Предполагает значения параметров **Максимум одновременных запросов** и `scan.workerpool.count` равными 10000 и 10, соответственно. Такая конфигурация требует около 6 ГБ оперативной памяти и загружает процессор на 40-50%. Применена по умолчанию.
- *Сбалансированная*. Предполагает значения параметров **Максимум одновременных запросов** и `scan.workerpool.count` равными 15000 и 10, соответственно. Такая конфигурация обеспечивает баланс между скоростью сканирования и потреблением ресурсов. Конфигурация требует около 6 ГБ оперативной памяти и загружает процессор на 40-50%.
- *Производительная*. Предполагает значения параметров **Максимум одновременных запросов** и `scan.workerpool.count` равными 10000 и 15, соответственно. Такая конфигурация обеспечивает высокую скорость сканирования, требует около 9 ГБ оперативной памяти и загружает процессор на 40-50% с пиками до 100%.

Для сохранения работоспособности решения произведение значений параметров **Максимум одновременных запросов** и `scan.workerpool.count` не должно превышать 150000.

а. Если необходимо, включите или выключите функцию **Обрабатывать результаты сразу после завершения задачи**. Если функция включена, служба фоновых задач обрабатывает результаты выполнения задачи сразу после ее завершения.

- **Для задачи Сканирование активов на соответствие профилям**

Для наглядного ознакомления с настройкой параметров задачи *Сканирование активов на соответствие профилям* вы можете просмотреть видео ниже.



В блоке **Профили соответствия** с помощью флажков выберите профили, на соответствие которым вы хотите проанализировать активы.

По кнопке **Обновить** вы можете принудительно обновить список отображающихся в задаче профилей соответствия. Без участия пользователя этот список синхронизируется со списком в разделе **Управление уязвимостями** → **Анализ соответствия** → **Только новые профили** с помощью фоновой задачи синхронизации.

С помощью переключателя **Показывать только выбранные профили** вы можете отобразить все имеющиеся профили соответствия или только выбранные.

10. На шаге **Настройка расписания запуска задачи** выберите вариант расписания.

11. Настройте дополнительные параметры задачи и расписания ее запуска.

Подробнее об этих параметрах групповой задачи см. в [справке Kaspersky Security Center](#).

12. В окне **Завершение создания задачи** нажмите на кнопку **Готово**.

Созданная задача отобразится в разделе **Задачи** в списке **Задачи** и будет передана службе фоновых задач Kaspersky Vulnerability Management после синхронизации с Сервером администрирования Kaspersky Security Center.

Согласно указанному расписанию или после ручного запуска пользователем служба фоновых задач будет запускать созданную задачу.

Значения по умолчанию для параметров запуска задач указаны в конфигурационном файле службы фоновых задач, который расположен в директории `/etc/kaspersky/vulnerability-management/configs/worker.json`.

Вы можете запускать и останавливать задачи в Kaspersky Security Center Web Console из списка задач в разделе **Задачи**.

Копирование, перемещение, приостановка и возобновление задач Kaspersky Vulnerability Management не поддерживаются.

Безагентное сканирование активов в режиме белого ящика

Безагентное сканирование в режиме белого ящика выполняется только на активах под управлением операционных систем семейства Linux.

С помощью групповой задачи Kaspersky Security Center *Безагентное сканирование в режиме белого ящика* Kaspersky Vulnerability Management выполняет сбор данных о программном обеспечении, установленном на активах, и поиск уязвимостей в нем. Для выполнения задачи требуется настройка доступа к данным активов с помощью учетной записи пользователя и не требуется установка на активах сканирующего агента.

Kaspersky Vulnerability Management подключается к активам под заранее созданной на активах учетной записью пользователя с помощью SSH-авторизации. Публичный и приватный ключи генерируются в процессе [установки компонентов решения](#).

Если в вашей организации предписана ротация SSH-ключей или SSH-ключи были скомпрометированы, вы можете обновить их.

Как обновить SSH-ключи

1. Любыми доступными средствами сгенерируйте пару публичного и приватного ключей. Имена файлов сертификатов с публичным и приватным ключами должны быть `whitebox.pub` и `whitebox.key`, соответственно.
2. Поместите сгенерированные ключи на активе с установленными компонентами решения в директорию `/etc/kaspersky/vulnerability-management/secrets/`.
3. Поместите сгенерированный публичный ключ на активы для сканирования в файл `authorized_keys`, расположенный в домашней директории учетной записи пользователя, созданной в процессе настройки задачи. Например, такой директорией может быть `/home/<user name>/.ssh`.

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.

Результаты сбора данных о программном обеспечении отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Программное обеспечение** отображается список приложений, установленных на активах, которые зарегистрированы в Kaspersky Vulnerability Management. При переходе по ссылке в названии приложения открывается карточка приложения, которая содержит описание приложения, информацию о найденных в приложении уязвимостях и об активах, на которых установлено приложение.
- В разделе **Управление уязвимостями** → **Уязвимости** в карточках уязвимостей на вкладке **Затронутое ПО** отображается список приложений, в которых обнаружены уязвимости. В разделе **Управление уязвимостями** → **Активы** в карточках устройств на вкладке **Установленное ПО** отображаются приложения, установленные на активах.

Результаты поиска уязвимостей отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Уязвимости** отображается список обнаруженных уязвимостей. При переходе по ссылке в названии уязвимости открывается [карточка уязвимости](#). В поле **Метод обнаружения** карточек уязвимостей отображается **Белый ящик**.
- В разделе **Управление уязвимостями** → **Активы** в карточках активов на вкладке **Обнаруженные уязвимости**. В поле **Метод обнаружения** карточек активов отображается **Белый ящик**.
- В разделе **Управление уязвимостями** → **Программное обеспечение** в карточках приложений на вкладке **Обнаруженные уязвимости**. В поле **Источник** карточек приложений отображается **Белый ящик**.

Безагентное сканирование активов в режиме черного ящика

Открытые порты могут использоваться злоумышленниками для проникновения в сеть и перехвата трафика, запуска атак. Службы, доступ к которым осуществляется через открытые порты, могут быть уязвимыми.

С помощью групповой задачи Kaspersky Security Center *Безагентное сканирование в режиме черного ящика* Kaspersky Vulnerability Management может выполнять следующие действия без установки агентов и без использования учетных данных на проверяемых активах (в режиме черного ящика):

- Искать на активах открытые порты и службы, доступные через открытые порты.
- Искать уязвимости в службах, доступных через открытые порты.

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.

Приложение, обеспечивающее безопасность актива, может определять сканирование актива в режиме черного ящика как сетевую атаку. В таком случае в настройках защитного приложения следует добавить IP-адрес устройства с установленными компонентами Kaspersky Vulnerability Management в исключения. Например, в Kaspersky Endpoint Security для Linux это нужно сделать в [настройках защиты от сетевых угроз](#).

Результаты выполнения задачи отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Уязвимости** отображается список обнаруженных уязвимостей. При переходе по ссылке в названии уязвимости открывается [карточка уязвимости](#). В поле **Метод обнаружения** карточек уязвимостей отображается **Черный ящик**.
- В разделе **Управление уязвимостями** → **Активы** в столбцах **Открытые порты** и **Сервисы** (не отображаются по умолчанию), в карточках активов на вкладках **Обнаруженные уязвимости** и **Сетевое сканирование**. В поле **Метод обнаружения** карточек активов отображается **Черный ящик**.
- В разделе **Управление уязвимостями** → **Программное обеспечение** в карточках приложений на вкладке **Обнаруженные уязвимости**. В поле **Источник** карточек приложений отображается **Черный ящик**.

Поиск уязвимостей в системном и прикладном ПО

Kaspersky Vulnerability Management выполняет поиск уязвимостей в зарегистрированном в базе данных ПО с помощью групповой задачи Kaspersky Security Center *Поиск уязвимостей*.

В рамках задачи *Поиск уязвимостей* Kaspersky Vulnerability Management выполняет поиск уязвимостей в следующих типах программного обеспечения: операционные системы, компоненты Windows, приложения, прошивки материнских плат активов и программные библиотеки.

После выполнения задачи Kaspersky Vulnerability Management выполняет перерасчет приоритета устранения для всех зарегистрированных в базе данных решения уязвимостей.

Результаты поиска уязвимостей отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Уязвимости** отображается список обнаруженных уязвимостей. При переходе по ссылке в названии уязвимости открывается [карточка уязвимости](#). В поле **Метод обнаружения** карточек уязвимостей отображается **Агент**.
- В разделе **Управление уязвимостями** → **Активы** в карточках активов на вкладке **Обнаруженные уязвимости**. В поле **Метод обнаружения** карточек активов отображается **Агент**.
- В разделе **Управление уязвимостями** → **Программное обеспечение** в карточках программного обеспечения на вкладке **Обнаруженные уязвимости**. В поле **Источник** карточек приложений отображается **Агент**.

Сканирование активов на соответствие профилям

Kaspersky Vulnerability Management выполняет анализ соответствия активов внутренним, отраслевым и регуляторным требованиям безопасности с помощью групповой задачи Kaspersky Security Center *Сканирование активов на соответствие профилям*.

Для выполнения задачи *Сканирование активов на соответствие профилям* необходимо, чтобы в Агентах администрирования Kaspersky Security Center, установленных на активах, была [включена функциональность Kaspersky Vulnerability Management](#).

В разделе **Управление уязвимостями** → **Анализ соответствия** → **Профили** отображаются данные о [профилях соответствия](#), [поставляемых с базами для модуля анализа соответствия](#) и [импортированные пользователем](#).

В настройках задачи *Сканирование активов на соответствие профилям* вы можете выбирать профили соответствия, предназначенные для операционных систем семейства Linux, даже если в области действия задачи выбраны активы под управлением операционных систем семейства Windows. И наоборот.

Результаты анализа активов на соответствие профилям отображаются в следующих разделах:

- В разделе **Управление уязвимостями – Анализ соответствия – Аудит соответствия**.
- В разделе **Управление уязвимостями – Активы** в карточках активов на вкладке **Анализ соответствия**.

Импорт пользовательских профилей соответствия

Профили соответствия поставляются с Kaspersky Vulnerability Management и, по умолчанию, [обновляются раз в сутки](#). Вы можете импортировать профили соответствия, [подготовленные в любом другом источнике](#).

Чтобы импортировать профили соответствия:

1. В главном окне Web Console выберите **Управление уязвимостями → Анализ соответствия → Профили**.
2. Нажмите на кнопку **Импортировать**.
3. В окне **Импортировать профили** загрузите ZIP-архив с XML-файлами профилей соответствия.

ZIP-архив должен содержать некоторое количество файлов *-oval.xml и файл *-xccdf.xml. Содержимое файла *-xccdf.xml должно быть в формате XCCDF.

4. Если в загружаемом архиве есть профили соответствия, которые уже были загружены ранее, выберите вариант импорта:
 - **Все профили.** Новые профили соответствия будут добавлены в список, ранее добавленные профили соответствия будут обновлены.
 - **Только новые профили.** Новые профили соответствия будут добавлены в список, ранее добавленные профили соответствия не будут обновлены.
5. Нажмите на кнопку **Импортировать**.

Импортированные профили соответствия отобразятся в таблице. При переходе по ссылке в названии профиля соответствия открывается карточка с данными профиля соответствия.

Примеры выбора типа сканирования для разных частей инфраструктуры

Многие организации имеют сложную ИТ-инфраструктуру: физические и виртуальные серверы, рабочие станции, облачные виртуальные машины, сетевые устройства. Для эффективной защиты важно правильно сопоставить методы сканирования уязвимостей с конкретными типами активов. Неверный выбор ведет либо к слепым зонам, либо к избыточной нагрузке на ИТ-инфраструктуру.

Kaspersky Vulnerability Management предлагает четыре типа сканирования, каждый из которых решает определенную задачу:

- Поиск уязвимостей:
 - Обнаруживает уязвимости в ОС, компонентах Windows, приложениях, библиотеках.
 - Не требует передачи учетных данных по сети.
 - Подходит для внутренних серверов, рабочих станций.
- Безагентное сканирование в режиме белого ящика:
 - Работает на активах под управлением операционных систем семейства Linux через SSH без установки агента.
 - Собирает данные об установленном программном обеспечении, выявляет уязвимости.
 - Требует настройки SSH-аутентификации по публичному ключу.
 - Подходит для Linux-активов, на которые нельзя установить Агент администрирования Kaspersky Security Center.
- Безагентное сканирование в режиме черного ящика:
 - Выполняет сканирование открытых портов и служб без использования учетных данных.
 - Оценивает инфраструктуру глазами злоумышленника.
 - Подходит для периметра сети, демилитаризованной зоны, сетевых устройств.
- Сканирование на соответствие профилям:
 - Выполняет проверку на соответствие требованиям безопасности.
 - Использует правила в форматах OVAL и XCCDF.
 - Подходит для регулируемого контура ИТ-инфраструктуры.

Рассмотрим организацию, ИТ-инфраструктура которой состоит из следующих частей:

- активы с доступом в Интернет;
- демилитаризованная зона с веб-серверами и обратными прокси;
- рабочие станции сотрудников;
- Linux-активы, на которые нельзя установить Агент администрирования Kaspersky Security Center;
- регулируемый контур, для которого требуется подтверждать выполнение требований безопасности.

Сотрудникам ИБ-команды необходимо организовать поиск уязвимостей в ИТ-инфраструктуре организации с помощью Kaspersky Vulnerability Management.

Рассмотрим далее примеры выбора типов сканирования.

Сканирование активов с доступом в Интернет

Из-за доступа активов в Интернет, безагентное сканирование в режиме черного ящика наиболее подходит для проверки данного периметра, так как в рамках этого сканирования решение может искать:

- открытые порты;
- доступные через них службы;
- уязвимости обнаруженных служб.

Для первичного аудита можно проверить все порты или использовать набор наиболее уязвимых. Для регулярного контроля рекомендуем ограничить задачу портами, которые должны быть открыты по утвержденной схеме публикации сервисов.

Сканирование активов в демилитаризованной зоне

В демилитаризованной зоне размещены веб-серверы, доступные из внешних или пограничных сетей. Для таких активов важно оценивать безопасность с двух сторон: с точки зрения того, что видно извне через сеть, и с точки зрения того, какое программное обеспечение установлено внутри серверов.

Поэтому для серверов в демилитаризованной зоне рекомендуется использовать комбинированный подход, объединяющий несколько взаимодополняющих типов сканирования.

В первую очередь целесообразно выполнять безагентное сканирование в режиме черного ящика. Этот тип проверки позволяет определить, какие порты и сетевые службы доступны на сервере, а также выявить уязвимости, связанные с обнаруженными службами. Такой подход имитирует внешний взгляд на актив и помогает понять, какие элементы серверной инфраструктуры потенциально доступны злоумышленнику через сеть.

Однако одного сканирования в режиме черного ящика недостаточно для полной оценки защищенности веб-серверов. Оно показывает только то, что можно обнаружить по сетевым признакам: открытые порты, службы и связанные с ними уязвимости. При этом часть установленного программного обеспечения может не быть доступна извне напрямую и, соответственно, не определяться таким способом.

Для анализа программного обеспечения внутри серверов следует дополнительно использовать один из двух вариантов:

- задачу поиска уязвимостей — если на серверах установлен Агент администрирования и сведения об установленном программном обеспечении уже поступают в базу данных Kaspersky Vulnerability Management;
- безагентное сканирование в режиме белого ящика — если установка Агента администрирования на серверах запрещена, но разрешено подключение к ним по SSH с использованием специальной учетной записи.

В результате для каждого сервера формируются два взаимодополняющих представления:

- Сетевое представление — какие порты и службы доступны на сервере, какие версии сервисов определяются извне и какие уязвимости связаны с сетевой поверхностью.
- Системное представление — какое программное обеспечение установлено внутри сервера и какие уязвимости связаны с операционной системой, пакетами, приложениями и библиотеками.

Такой комбинированный подход позволяет более полно оценить состояние безопасности серверов в демилитаризованной зоне. Он снижает риск пропустить уязвимости, которые присутствуют на сервере, но не видны при сканировании в режиме черного ящика, и одновременно помогает контролировать внешнюю поверхность атаки, доступную через сеть.

Сканирование рабочих станций сотрудников

На рабочих станциях сотрудников установлен Агент администрирования, поэтому такие активы уже находятся под централизованным управлением и регулярно передают в Kaspersky Vulnerability Management сведения, необходимые для анализа защищенности. В частности, в решение поступает информация об установленном программном обеспечении, операционной системе, версиях приложений и других параметрах, на основании которых можно определить наличие известных уязвимостей.

Для этого сценария наиболее подходящим типом проверки является поиск уязвимостей. Поиск уязвимостей ориентирован на массовое и регулярное сканирование управляемых активов, по которым в базе данных решения уже есть инвентаризационная информация. Нет необходимости дополнительно выполнять сетевое сканирование или настраивать отдельный доступ к каждому устройству. Достаточно использовать задачу поиска уязвимостей, которая анализирует уже собранные данные и сопоставляет их с базой известных уязвимостей.

Сканирование активов, на которые нельзя установить Агент администрирования

В организации есть активы под управлением операционных систем семейства Linux, на которые по требованиям эксплуатации нельзя устанавливать Агент администрирования. При этом для целей аудита безопасности допускается использование специальной учетной записи с необходимыми правами доступа.

Для таких активов наиболее подходящим типом сканирования является безагентное сканирование в режиме белого ящика. Этот режим позволяет подключаться к активам без установки Агента администрирования, собирать сведения об установленном программном обеспечении и выявлять связанные с ним уязвимости.

Использование других типов сканирования в данном сценарии менее эффективно. Например, безагентное сканирование в режиме черного ящика позволяет обнаружить открытые порты, доступные сетевые службы и потенциальные уязвимости этих служб, но не предоставляет полной информации о программном обеспечении, установленном на активе. Поэтому такой режим больше подходит для оценки сетевой поверхности атаки, а не для полноценного анализа программного обеспечения на Linux-активах.

Задача поиска уязвимостей также не является первичным вариантом для таких активов, поскольку она работает с программным обеспечением, которое уже зарегистрировано в базе данных решения. Если Агент администрирования на активе не установлен, сведения об установленном программном обеспечении не поступают автоматически через Агент администрирования. Следовательно, перед использованием задачи поиска уязвимостей эти данные необходимо получить другим способом.

В рассматриваемом сценарии таким способом является безагентное сканирование в режиме белого ящика. Оно позволяет сначала собрать информацию об установленном программном обеспечении на Linux-активах, а затем использовать эти данные для выявления и дальнейшей обработки уязвимостей в Kaspersky Vulnerability Management.

Анализ соответствия требованиям безопасности в регулируемом контуре

В регулируемом контуре перед ИБ-командой стоит задача не только выявлять уязвимости в операционных системах и программном обеспечении, но и регулярно подтверждать, что конфигурации активов соответствуют установленным требованиям безопасности. К таким требованиям могут относиться внутренние стандарты по усилению защиты, отраслевые практики, требования регуляторов, а также специальные профили безопасности, применимые к конкретным типам операционных систем.

Для этого сценария рекомендуется использовать сканирование активов на соответствие профилям. В отличие от обычного поиска уязвимостей, такая проверка ориентирована не на сопоставление установленного программного обеспечения с базой известных уязвимостей, а на анализ конфигурации актива по заранее определенному набору правил.

Итоговые рекомендации

Тип сканирования следует выбирать не только по типу актива, но и по поставленной задаче:

- требуется проверить на уязвимости периметр снаружи — безагентное сканирование в режиме черного ящика;
- требуется проверить на уязвимости установленное программное обеспечение Linux-активов без Агента администрирования — безагентное сканирование в режиме белого ящика;
- требуется выявить уязвимости в программном обеспечении активов, зарегистрированном в базе данных решения — поиск уязвимостей;
- требуется подтвердить выполнение требований безопасности — сканирование на соответствие профилям.

Не следует пытаться охватить всю инфраструктуру одной задачей. Разделение по сетевым зонам, операционным системам, способу управления и требованиям безопасности делает результаты точнее, а нагрузку и доступы — контролируемыми.

Анализ и приоритизация уязвимостей

В этом разделе дана информация о карточках уязвимостей и работе с отчетами, с помощью которых вы можете анализировать и приоритизировать уязвимости.

Просмотр найденных уязвимостей

Уязвимости, обнаруженные в результате сканирования, отображаются в следующих разделах:

- В разделе **Управление уязвимостями** → **Уязвимости** отображается список обнаруженных уязвимостей. При переходе по ссылке в названии уязвимости открывается карточка уязвимости. Вы можете настраивать отображение списка уязвимостей с помощью кнопок над списком уязвимостей:
 - **Группировка по уязвимостям.** В списке отображаются уникальные уязвимости. Для каждой уязвимости отображаются все активы и программное обеспечение, которые затрагивает уязвимость.
 - **Без группировки.** В списке отображаются уникальные комбинации уязвимости, затронутого актива и затронутого программного обеспечения. В таком списке одна и та же уязвимость может присутствовать несколько раз.
- В разделе **Управление уязвимостями** → **Активы** в карточках активов на вкладке **Обнаруженные уязвимости**.
- В разделе **Управление уязвимостями** → **Программное обеспечение** в карточках программного обеспечения на вкладке **Обнаруженные уязвимости**.

При переходе по ссылке с названием уязвимости открывается карточка уязвимости. В зависимости от способа отображения списка уязвимостей (**Группировка по уязвимостям** / **Без группировки**) в карточке уязвимости могут быть отражены следующие данные:

- Название уязвимости.
- Данные активов и ПО, которые затронула уязвимость – при отображении списка уязвимостей с группировкой по уязвимостям. [Приоритет устранения](#) , рассчитанный по [методике ФСТЭК](#) , данные актива и ПО, которые затронула уязвимость – при отображении списка уязвимостей без группировки.
- Идентификатор уязвимости в базе угроз и уязвимостей "Лаборатории Касперского", описание от "Лаборатории Касперского" и описание уязвимости от поставщика данных об уязвимости (если имеется).

Описание уязвимости от поставщика данных об уязвимости переносится без проверки на точность и полноту, изменений и сокращений со стороны "Лаборатории Касперского".

- Внешние идентификаторы уязвимости.
- Дата публикации и метод(ы) обнаружения уязвимости – при отображении списка уязвимостей с группировкой по уязвимостям. Дата публикации описания уязвимости во внешнем источнике, дата и время первого обнаружения уязвимости, дата и время последнего обнаружения уязвимости и метод(ы) обнаружения уязвимости – при отображении списка уязвимостей без группировки.
- [Уровень опасности](#)  и оценки согласно стандартам CVSS v2, CVSS v3 и CVSS v4.

- Данные о рисках эксплуатации уязвимости, в том числе [вероятность EPSS](#) и [процентиль EPSS](#).
- Рекомендуемые действия для устранения уязвимости.
- Ссылки на публичные источники, в которых описана уязвимость или уязвимости такого типа.

Работа с отчетами

Отчеты представляют данные, полученные в результате работы Kaspersky Vulnerability Management, в структурированном и наглядном виде. С помощью отчетов вы можете анализировать данные для оценки защищенности ИТ-инфраструктуры организации и принятия управленческих решений.

Любой отчет генерируется на основе шаблона отчета. Шаблоны отчетов бывают предустановленными и пользовательскими.

Вы можете управлять отчетами и шаблонами отчетов в разделе **Управление уязвимостями** → **Отчеты** на вкладках **Отчеты** и **Шаблоны**.

Создание и редактирование шаблонов отчетов

Вы можете выполнять следующие действия с шаблонами отчетов.

Как создать шаблон отчета

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.

2. Перейдите на вкладку **Шаблоны**.

3. Нажмите на кнопку **Добавить**.

Откроется Мастер создания шаблона отчета. Для перехода к следующему шагу используйте кнопку **Далее**.

4. Задайте основные настройки шаблона отчета:

a. Выберите тип шаблона отчета:

- **Отчет об уязвимостях.**
- **Отчет об активах.**

b. Введите название шаблона отчета.

c. Если необходимо, с помощью флажка **Сгенерировать отчет после создания шаблона** включите функцию генерации отчета после создания шаблона.

5. Задайте область сбора данных для отчетов, которые будут генерироваться на основе шаблона, одним из следующих способов:

- в блоке **Сканировать** выберите **Выбранные активы** и сформируйте список активов, данные которых будут отображаться в отчетах на основе создаваемого шаблона:

a. Нажмите на кнопку **Добавить активы**.

b. В открывшемся окне **Добавление активов** выберите активы.

c. Нажмите на кнопку **Сохранить**.

Выбранные активы отобразятся в таблице на шаге **Область сбора данных**.

- в блоке **Сканировать** выберите **Все активы** – в отчетах на основе создаваемого шаблона будут отображаться данные всех активов, зарегистрированных в базе данных решения на момент формирования отчета.

6. Задайте настройки для представления данных в отчетах, которые будут генерироваться на основе шаблона отчета:

a. Добавляйте и удаляйте столбцы отчета с помощью одноименных кнопок.

b. Включайте и выключайте сортировку данных по столбцам и фильтрацию данных в столбцах с помощью кнопки **Редактировать**.

7. Нажмите на кнопку **Сохранить**.

Созданный шаблон отчета отобразится на вкладке **Шаблоны**.

Как создать шаблон отчета с помощью копирования имеющегося шаблона отчета

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.

2. Перейдите на вкладку **Шаблоны**.

3. Выберите шаблон отчета с помощью флажка около названия шаблона.

4. Нажмите на кнопку **Копировать**.

Откроется Мастер создания шаблона отчета с настройками копируемого шаблона отчета. Для перехода к следующему шагу используйте кнопку **Далее**.

5. Если необходимо, измените основные настройки шаблона отчета, за исключением типа шаблона отчета.

6. Если необходимо, измените область сбора данных для отчетов, которые будут генерироваться на основе шаблона.

7. Если необходимо, измените настройки для представления данных в отчетах, которые будут генерироваться на основе шаблона.

8. Нажмите на кнопку **Сохранить**.

Созданный шаблон отчета отобразится на вкладке **Шаблоны**.

Как редактировать шаблон отчета

1. Перейдите к свойствам шаблона отчета любым из доступных способов.

- На вкладке **Шаблоны**:
 - a. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
 - b. Перейдите на вкладку **Шаблоны**.
 - c. Перейдите по ссылке в названии шаблона отчета.
- На вкладке **Отчеты**:
 - a. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
 - b. Перейдите на вкладку **Отчеты**.
 - c. Выберите отчет с помощью флажка слева от его названия.
 - d. Нажмите на кнопку **Перейти к шаблону** в верхней части таблицы.

Если шаблон отчета был удален, кнопка **Перейти к шаблону** недоступна.

- Из отчета:
 - a. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
 - b. Перейдите на вкладку **Отчеты**.
 - c. Перейдите по ссылке в названии отчета.
 - d. В открывшемся отчете нажмите на кнопку **Перейти к шаблону** в левом верхнем углу.

Если шаблон отчета был удален, кнопка **Перейти к шаблону** недоступна.

2. В открывшемся окне с настройками шаблона отчета внесите необходимые изменения.

3. В окне с настройками шаблона отчета нажмите на кнопку **Сохранить**.

Формирование отчетов на основе шаблонов

На основе шаблонов отчетов вы можете генерировать отчеты следующими способами.

Как сгенерировать отчет сразу после создания шаблона отчета

1. На шаге **Основная информация** при создании или редактировании шаблона отчета установите флажок **Сгенерировать отчет после создания шаблона**.
2. Настройте шаблон отчета в соответствии с шагами мастера.

3. На шаге **Представление данных** при создании или редактировании шаблона отчета нажмите на кнопку **Сохранить**.

На основе сохраненного шаблона отчета будет сгенерирован отчет.

Как запустить генерацию отчетов на вкладке **Шаблоны**

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
2. Перейдите на вкладку **Шаблоны**.
3. Выберите один или несколько шаблонов отчетов с помощью флажков слева от их названий.
4. Нажмите на кнопку **Сгенерировать** в верхней части таблицы.

На основе выбранных шаблонов отчетов будут сгенерированы отчеты.

Как запустить генерацию отчета в свойствах шаблона отчета

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
2. Перейдите на вкладку **Шаблоны**.
3. Нажмите на ссылку на названии шаблона отчета, на основе которого вы хотите сгенерировать отчет.
4. На вкладке **Основная информация** нажмите на кнопку **Сгенерировать**.

Сгенерированные отчеты отобразятся на вкладке **Отчеты** и в свойствах соответствующих шаблонов отчетов на вкладке **Основная информация** в блоке **Сгенерированные отчеты**.

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.

По умолчанию сгенерированные отчеты хранятся в базе данных решения в течение 30 суток. Время, оставшееся до удаления отчета, отображается на вкладке **Отчеты** в таблице отчетов в столбце **Удаление через**. Вы можете изменить продолжительность хранения отчетов в базе данных решения с помощью [конфигурационного файла](#). Сохраненные отчеты могут понадобиться на этапе [контроля устранения уязвимостей](#).

Если необходимо, вы можете остановить генерацию отчета на вкладке **Отчеты** с помощью кнопки **Остановить** в верхнем левом углу таблицы отчетов.

Экспорт отчетов

Вам может понадобиться экспортировать отчеты в файлы, чтобы предоставить их руководству или другим заинтересованным лицам, не имеющим доступа к Kaspersky Vulnerability Management, а также для [контроля устранения уязвимостей](#).

Как экспортировать отчеты на вкладке **Отчеты**

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
2. Перейдите на вкладку **Отчеты**.

3. С помощью флажков слева от названий отчетов выберите один или несколько отчетов.
4. В раскрывающемся меню кнопки **Экспортировать** выберите формат, в который вы хотите экспортировать отчеты, – XLSX или JSON.
Откроется окно для сохранения отчета или архива, если вы экспортируете несколько отчетов.
5. Если необходимо, скорректируйте название отчета или архива.
6. Укажите путь, по которому будет сохранен файл отчета или архив.
7. Нажмите на кнопку **Сохранить**.

Как экспортировать отчет из свойств отчета

1. В главном окне Web Console выберите **Управление уязвимостями → Отчеты**.
2. Перейдите на вкладку **Отчеты**.
3. Перейдите по ссылке в названии нужного отчета.
Откроется выбранный отчет.
4. В раскрывающемся меню кнопки **Экспортировать** выберите формат файла, в который вы хотите экспортировать отчет, – XLSX или JSON.
Откроется окно для сохранения отчета.
5. Если необходимо, скорректируйте название отчета.
6. Укажите путь, по которому будет сохранен файл отчета.
7. Нажмите на кнопку **Сохранить**.

Экспорт отчетов не работает при количестве записей более одного миллиона. Для решения проблемы мы рекомендуем уменьшать число полей (столбцов) в отчете.

Удаление отчетов и шаблонов отчетов

Как удалить отчеты на вкладке Отчеты

1. В главном окне Web Console выберите **Управление уязвимостями → Отчеты**.
2. Перейдите на вкладку **Отчеты**.
3. Выберите один или несколько отчетов с помощью флажков слева от их названий.
4. Нажмите на кнопку **Удалить** в верхней части таблицы.

Как удалить отчеты в свойствах шаблона отчета

1. В главном окне Web Console выберите **Управление уязвимостями → Отчеты**.
2. Перейдите на вкладку **Шаблоны**.

3. Нажмите на ссылку на названии шаблона, отчеты которого вы хотите удалить.
4. На вкладке **Основная информация** в блоке **Сгенерированные отчеты** установите флажки около названий отчетов, которые вы хотите удалить.
5. Нажмите на кнопку **Удалить**.

Как удалить шаблоны на вкладке **Шаблоны**

1. В главном окне Web Console выберите **Управление уязвимостями** → **Отчеты**.
2. Перейдите на вкладку **Шаблоны**.
3. Выберите один или несколько шаблонов отчетов с помощью флажков слева от их названий.
4. Нажмите на кнопку **Удалить** в верхней части таблицы.

Работа с данными отчетов

Данные, представленные в отчете, зависят от типа отчета.

Отчет об уязвимостях содержит список уязвимостей, обнаруженных на указанных в шаблоне отчета активах, распространенность найденных уязвимостей по ИТ-инфраструктуре организации. Также отчет об уязвимостях содержит следующие гистограммы:

- Количество уязвимостей по каждому уровню опасности.
- Наиболее опасные по оценке CVSS v3 уязвимости.
- Наиболее распространенные уязвимости.

Отчет об активах содержит список активов, на которых обнаружены уязвимости, с подробными данными об обнаруженных уязвимостях. Также отчет об активах содержит следующие гистограммы:

- Количество активов с обнаруженными уязвимостями для каждого уровня значимости актива.
- Активы с наибольшим количеством обнаруженных уязвимостей.

Вы можете выполнять следующие действия с данными отчетов:

- [Экспортировать](#) один или несколько отчетов в файлы.
- Искать данные в отчете. В строке поиска над таблицей отчета введите текст и нажмите на значок .
- Сортировать данные отчета. Нажмите на название нужного столбца таблицы отчета, и данные отчета будут отсортированы по значениям выбранного столбца.

Сценарий: приоритизация уязвимостей с учетом значимости активов

Рассмотрим подход к управлению уязвимостями, который помогает выстроить обоснованную последовательность их устранения и эффективнее использовать ресурсы ИТ- и ИБ-команд.

Kaspersky Vulnerability Management позволяет определить, какие уязвимости требуют первоочередного внимания. Применяемая в решении [методика ФСТЭК](#) ² дополняет техническую оценку CVSS *контекстом ИТ-инфраструктуры организации*. Согласно действующей методике ФСТЭК, при определении приоритета устранения уязвимости учитываются следующие параметры:

- оценка уязвимости по CVSS;
- тип и количество затронутых активов;
- влияние затронутых активов на защищенность ИТ-инфраструктуры организации;
- сведения об эксплуатации уязвимости и наличии эксплойта;
- возможные последствия эксплуатации.

Вам не нужно самостоятельно оценивать множество характеристик уязвимости. Формула расчета методики ФСТЭК и единые весовые коэффициенты снижают влияние субъективных экспертных оценок. Использование единого подхода методики упрощает обоснование и планирование работ по устранению уязвимостей.

Для приоритизации уязвимостей с учетом значимости активов предлагаем следующие этапы.

Определение значимости активов

Для каждого актива должна быть указана значимость:

- *Критичная* — нарушение работы или компрометация актива может привести к остановке критически важных процессов, масштабному нарушению безопасности, невозможности восстановления инфраструктуры в приемлемые сроки.
- *Высокая* — инцидент может существенно повлиять на отдельные системы или бизнес-процессы, привести к утечке защищаемой информации либо создать условия для дальнейшего развития атаки.
- *Средняя* — последствия ограничены отдельным подразделением, сервисом или группой пользователей и могут быть устранены в рамках штатных процедур.
- *Низкая* — актив оказывает незначительное влияние на работу организации, не обрабатывает критичную информацию и не предоставляет существенных возможностей для развития атаки.
- *Не определена* — оценка еще не выполнена либо для нее недостаточно сведений.

Определение значимости позволяет учитывать роль каждого актива в ИТ-инфраструктуре организации и возможные последствия его компрометации при расчете приоритета устранения уязвимостей. Благодаря этому ИТ- и ИБ-команды могут сосредоточить ресурсы на активах, защита которых дает наибольший эффект: поддерживает непрерывность ключевых процессов, ограничивает развитие атак и снижает вероятность масштабного ущерба.

В первую очередь необходимо определить значимость, например, следующих категорий активов:

- контроллеры домена и другие системы управления учетными записями;
- активы с развернутыми средствами централизованного управления ИТ-инфраструктурой;
- рабочие станции администраторов и других привилегированных пользователей;
- точки входа во внутреннюю ИТ-инфраструктуру;
- активы, участвующие в обеспечении критичных бизнес-процессов;
- активы, от которых зависит работа большого количества других систем;
- системы резервного копирования и хранения резервных копий;
- активы, доступные из интернета или других недоверенных сетей;
- активы, на которых хранятся или обрабатываются персональные данные и иная защищаемая информация.

Эти категории требуют первоочередной оценки, поскольку их компрометация может иметь последствия, значительно превышающие ущерб от нарушения работы одного устройства или сервиса. Такие активы могут предоставлять привилегированный доступ, использоваться для централизованного распространения изменений, обеспечивать работу множества зависимых систем или служить точкой входа во внутреннюю ИТ-инфраструктуру организации.

Сортировка уязвимостей по приоритету устранения

После определения значимости активов Kaspersky Vulnerability Management рассчитывает приоритет устранения обнаруженных уязвимостей по методике ФСТЭК.

Отсортируйте список обнаруженных уязвимостей по значению приоритета устранения:

1. В главном окне Web Console перейдите в раздел **Управление уязвимостями** → **Уязвимости**.
2. В таблице уязвимостей без группировки нажмите на заголовок столбца **Приоритет устранения**.
3. В раскрывшемся меню выберите тип сортировки **По убыванию**.

Уязвимости будут расположены в следующем порядке:

- *Критичный* приоритет;
- *Высокий* приоритет;
- *Средний* приоритет;

- *Низкий* приоритет;
- приоритет *Не определен*.

Формирование очереди уязвимостей для устранения

При формировании очереди на устранение уязвимостей рекомендуем использовать риск-ориентированный подход. Его задача — направить ресурсы ИТ- и ИБ-команд на уязвимости, эксплуатация которых может привести к наиболее существенным последствиям для организации. При таком подходе следует сортировать уязвимости по приоритету устранения, который учитывает их техническую опасность и контекст ИТ-инфраструктуры, включая значимость затронутого актива. Такой подход позволяет последовательно снижать наиболее существенные риски и рационально распределять доступные ресурсы.

При формировании очереди уязвимостей для устранения рекомендуем руководствоваться следующими правилами:

- Уязвимости с критичным приоритетом устранения необходимо устранять в первую очередь. Для них следует назначить ответственных, определить минимально возможные сроки и контролировать выполнение работ до полного устранения риска.
- Уязвимости с высоким приоритетом устранения необходимо устранять в текущем цикле устранения. Их обработку рекомендуем планировать сразу после критичных уязвимостей, не перенося на последующие циклы без обоснованной причины.
- Уязвимости со средним или низким приоритетом устранения необходимо устранять планово, если отсутствуют дополнительные повышающие факторы. Такие работы удобно объединять с регулярным обновлением систем и другими задачами по сопровождению ИТ-инфраструктуры.
- Для уязвимостей с неопределенным приоритетом устранения необходимо проверить полноту исходных данных и добиться расчета приоритета. До завершения анализа такие уязвимости не следует помещать в конец очереди автоматически.

Очередь необходимо регулярно пересматривать при появлении новых сведений об уязвимостях, изменении значимости активов или конфигурации ИТ-инфраструктуры. Если устранить уязвимость в установленный срок невозможно, следует применить компенсирующие меры, зафиксировать принятое решение и определить срок повторной оценки.

Таким образом, сортировка по приоритету превращает общий перечень уязвимостей в понятный и управляемый план работ. Организация получает возможность сначала устранять угрозы с наибольшим потенциальным влиянием, обоснованно планировать нагрузку специалистов и последовательно снижать риски для ключевых систем и бизнес-процессов.

Устранение уязвимостей

На этом этапе следует принимать меры по устранению или исключению возможности использования уязвимостей.

Этап подразумевает следующие активности:

1. Согласование установки обновлений уязвимых приложений с ИТ-департаментом.
2. Формирование плана установки обновлений.
3. Тестирование обновлений.
4. Установка обновлений с помощью Kaspersky Security Center:
 - a. Для каждого из уязвимых приложений в Kaspersky Security Center Web Console создайте групповую задачу *Удаленная установка приложения* с инсталляционным пакетом обновленной версии приложения с устраненной уязвимостью.
Подробнее о создании задачи *Удаленная установка приложения* см. в [справке Kaspersky Security Center](#) .
 - b. Запустите созданные задачи *Удаленная установка приложения*.
5. Разработка компенсирующих мер защиты.

Контроль устранения уязвимостей

На этом этапе следует анализировать данные об устранении уязвимостей.

Этап подразумевает следующие активности:

1. Генерация отчетов об активах и/или уязвимостях и [экспорт отчетов](#).
2. Обновление сгенерированных ранее отчетов через установленное для устранения уязвимостей время и экспорт отчетов.
3. Сравнение экспортированных отчетов и оценка устранения уязвимостей.

Администрирование

В этом разделе описаны известные ограничения и приведены инструкции по расширенной настройке и удалению решения.

Известные ограничения

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

- [8330927] Для некоторых уязвимостей, обнаруженных в результате выполнения задачи *Безагентное сканирование в режиме черного ящика*, отображается только ограниченная информация.
- [8609559] Не поддерживаются копирование, перемещение, приостановка и возобновление [задач Kaspersky Vulnerability Management](#).
- [9512558] В карточках приложений, установленных на активах под управлением операционных систем Linux, на вкладке **Установлено на активах** не заполняется поле **Путь к файлу**.
- [10736272] Не поддерживаются группы активов для формирования области сбора данных для отчетов.
- [9180441] Область действия роли для Kaspersky Vulnerability Management не ограничена, даже если в области действия роли добавлены комбинации групп администрирования и пользователей.
- [9180441] 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.
- [9344429] В свойствах задач Kaspersky Vulnerability Management на вкладке **Результаты** для событий о статусе задачи *Завершена с предупреждением* не заполняется поле **Описание**.
- [9380569] Сканирование в режиме белого ящика возможно только на активах под управлением операционных систем семейства Linux.
- [9320676] 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.
- [9565353] 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.
- [9648166] Информация о производителе и версии прошивки материнской платы собирается только для ограниченного набора устройств.
- [10736890] Обновить решение с версии 1.0 до версии 1.1 можно только удалив предыдущую версию и установив новую.

Обновление с версии 1.0 до версии 1.1

Обновление Kaspersky Vulnerability Management с версии 1.0 до версии 1.1 состоит из следующих этапов:

- 1 **Сохранение SSH-ключей, которые используются для безагентного сканирования в режиме белого ящика**

Создайте резервную копию приватного ключа `whitebox.key` и публичного ключа `whitebox.pub`, расположенных в директории `/etc/kaspersky/vulnerability-management/secrets/`.

- 2 **Удаление компонентов Kaspersky Vulnerability Management версии 1.0**

- 3 **Обновление Сервера администрирования, Web Console и Агента администрирования Kaspersky Security Center Linux версии 16.3 до версии 17**

Подробнее об обновлении см. в [справке Kaspersky Security Center](#).

- 4 **Обновление веб-плагина для управления решением до версии 1.1**

- 5 **Установка и настройка компонентов Kaspersky Vulnerability Management версии 1.1**

В процессе установки вводите данные для подключения к базе данных, которая была создана для Kaspersky Vulnerability Management версии 1.0.

- 6 **Восстановление SSH-ключей, сохраненных на первом этапе сценария**

Поместите приватный ключ `whitebox.key` и публичный ключ `whitebox.pub`, сохраненные на первом этапе сценария, в директорию `/etc/kaspersky/vulnerability-management/secrets/`.

Установка веб-плагина для управления решением

На устройстве с установленным Kaspersky Security Center Web Console необходимо обновить веб-плагин для управления решением.

Чтобы обновить веб-плагин для управления решением через Kaspersky Security Center Web Console:

1. В главном окне Web Console выберите **Параметры → Веб-плагины**.

Откроется список установленных веб-плагинов.

2. Выберите **Kaspersky Vulnerability Management**.

3. Нажмите на кнопку **Обновить из файла**.

4. В открывшемся окне загрузите архив с дистрибутивом веб-плагина `vulnerability_management.zip` и файл с подписью `signature.txt`. Эти файлы упакованы в архив `webconsole-plugin.zip`.

Архив `webconsole-plugin.zip` входит в [комплект поставки](#).

5. Нажмите на кнопку **Обновление**.

6. Дождитесь окончания обновления и нажмите на кнопку **ОК** в информационном окне.

Новый плагин отобразится в списке установленных веб-плагинов в разделе **Параметры → Веб-плагины**.

Обновление баз уязвимостей

Функциональность обновлений и KSN может быть недоступна в решении на территории США.

Базы уязвимостей для Kaspersky Vulnerability Management обновляются с помощью следующих поставщиков:

- Обновления баз для модуля обнаружения программного обеспечения предоставляет Сервер администрирования Kaspersky Security Center.
- Обновления баз для Сетевого сканера, модулей обнаружения уязвимостей и анализа соответствия предоставляет служба обновления баз решения.

Вы можете изменять [источник для обновления баз уязвимостей](#) и [периодичность обновления баз уязвимостей](#).

Настройка источника для обновления баз уязвимостей

Чтобы настроить источник для обновления баз уязвимостей с помощью помощника по настройке:

1. На устройстве с установленными компонентами Kaspersky Vulnerability Management откройте терминал.
2. Запустите помощника по настройке Kaspersky Vulnerability Management:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh updatemode
```

3. Помощник по настройке отобразит текущий источник обновлений и предложит изменить его.
4. Укажите тип источника обновлений:

- **KasperskyLabSecure**. Обновления баз поставляются с серверов обновлений "Лаборатории Касперского".

Выбирайте этот тип источника, если устройство с установленными компонентами Kaspersky Vulnerability Management имеет возможность подключаться по сети к внешним источникам обновлений.

- **LocalTrusted**. Обновления баз поставляются из локальной или смонтированной директории на устройстве, задаваемой с помощью дополнительного параметра **urls**.

Выбирайте этот тип источника, если устройство с установленными компонентами Kaspersky Vulnerability Management не имеет возможности подключаться по сети к внешним источникам обновлений. Например, если устройство находится в закрытом сегменте корпоративной сети.

5. Если вы указали тип источника обновлений `LocalTrusted`, введите путь к локальной директории или смонтированной директории на устройстве с установленным Kaspersky Vulnerability Management в формате `/path/to/dir`.

В локальную или смонтированную директорию базы уязвимостей необходимо [загружать с помощью Kaspersky Update Utility](#).

Чтобы настроить источник для обновления баз уязвимостей с помощью конфигурационных файлов:

1. Откройте конфигурационный файл нужного компонента, расположенный в директории `/etc/kaspersky/vulnerability-management/configs/`:

- для Сетевого сканера – файл `updater-scanner.json`;
- для модуля обнаружения уязвимостей – файл `vms.json`;
- для модуля анализа соответствия – файл `updater-compliance.json`.

Для просмотра конфигурационных файлов требуются права группы операционной системы `root` или [kvm-group](#). Для изменения конфигурационных файлов требуются права группы `root`.

2. Укажите тип источника обновлений с помощью значения параметра `type`:

- `KasperskyLabSecure`. Обновления баз поставляются с серверов обновлений "Лаборатории Касперского".

Выбирайте этот тип источника, если устройство с установленными компонентами Kaspersky Vulnerability Management имеет возможность подключаться по сети к внешним источникам обновлений.

- `LocalTrusted`. Обновления баз поставляются из локальной или смонтированной директории на устройстве, задаваемой с помощью дополнительного параметра `urls`.

Выбирайте этот тип источника, если устройство с установленными компонентами Kaspersky Vulnerability Management не имеет возможности подключаться по сети к внешним источникам обновлений. Например, если устройство находится в закрытом сегменте корпоративной сети.

3. Если вы указали тип источника обновлений `LocalTrusted`, введите путь к локальной директории или смонтированной директории на устройстве с установленным Kaspersky Vulnerability Management в формате `/path/to/dir`.

В локальную или смонтированную директорию базы уязвимостей необходимо [загружать с помощью Kaspersky Update Utility](#).

4. Сохраните изменения в конфигурационных файлах.

5. Перезапустите компоненты решения:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh restart
```

Изменение периодичности обновления баз уязвимостей

Чтобы изменить периодичность обновления баз уязвимостей:

1. Откройте конфигурационный файл нужного компонента, расположенный в директории `/etc/kaspersky/vulnerability-management/configs/`:

- для Сетевого сканера и модуля анализа соответствия – файл `privateapi.json`;
- для модуля обнаружения уязвимостей – файл `vms.json`.

Для просмотра конфигурационных файлов требуются права группы операционной системы `root` или [kvm-group](#). Для изменения конфигурационных файлов требуются права группы `root`.

2. Измените значение параметра, отвечающего за периодичность обновления баз уязвимостей:

- `updater.interval` – периодичность обновления баз в часах для Сетевого сканера и модуля анализа соответствия;
- `updater.intervalInHours` – периодичность обновления баз в часах для модуля обнаружения уязвимостей.

3. Сохраните изменения в конфигурационных файлах.

4. Перезапустите компоненты решения:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh restart
```

Загрузка баз уязвимостей с помощью Kaspersky Update Utility

Если устройство с установленными компонентами Kaspersky Vulnerability Management не имеет возможности подключаться по сети к внешним источникам для обновления баз уязвимостей, вы можете загружать базы уязвимостей с помощью Kaspersky Update Utility.

Чтобы загрузить обновления баз уязвимостей с помощью Kaspersky Update Utility:

1. На устройство с доступом в интернет загрузите дистрибутив Kaspersky Update Utility с [веб-сайта Службы технической поддержки "Лаборатории Касперского"](#).
2. Установите Kaspersky Update Utility.
3. Запустите Kaspersky Update Utility.

4. Настройте параметры Kaspersky Update Utility:

- a. В качестве способа обновления выберите **Список программ**.
- b. В списке программ выберите Kaspersky Vulnerability Management 1.1.
- c. Укажите директорию, в которую Kaspersky Update Utility будет скачивать базы уязвимостей.

5. Запустите скачивание баз уязвимостей.

Базы уязвимостей будут скачаны в директорию, указанную в пункте 4с инструкции.

6. Удобным вам способом перенесите скачанные базы уязвимостей на устройство с установленными компонентами Kaspersky Vulnerability Management в директорию, указанную с помощью параметра `urls` при [настройке источника обновления баз уязвимостей](#).

Шаги инструкции обозначены схематично. Подробнее о работе с Kaspersky Update Utility см. в [Базе знаний "Лаборатории Касперского"](#).

Расширенная настройка решения с помощью конфигурационных файлов

В конфигурационных файлах, расположенных в директории `/etc/kaspersky/vulnerability-management/configs/`, вы можете настроить те параметры решения, которые недоступны для настройки в [интерфейсе решения](#). Вы можете изменять имеющиеся или добавлять отсутствующие параметры, описанные в статьях ниже.

Для просмотра конфигурационных файлов требуются права группы операционной системы `root` или `kvm-group`. Для изменения конфигурационных файлов требуются права группы `root`.

Для применения изменений в конфигурационных файлах необходимо перезапустить службы решения:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh restart
```

privateapi.json

С помощью конфигурационного файла `privateapi.json` вы можете настраивать параметры службы [Private API](#).

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {
  "source.priority": ""
}
```

Параметры конфигурационного файла `privateapi.json`

Параметр	Описание
<code>http.server.allowedorigins</code>	Определяет, с каких доменов могут быть отправлены запросы к Private API.
<code>http.server.host</code>	URL-адрес сервера, на котором установлен компонент Private API.
<code>http.server.port</code>	Номер порта для доступа к серверу, на котором установлен компонент Private API.
<code>http.server.tls.enable</code>	Параметр определяет использование SSL для подключения к Private API. Возможные значения: <code>true</code> или <code>false</code> .
<code>http.server.tls.servercertfile</code>	Путь к файлу с TLS-сертификатом для Private API.
<code>http.server.tls.serverkey</code>	Путь к файлу с ключом TLS-сертификата для доступа к Private API.
<code>http.auth.methods</code>	Тип аутентификации для доступа к Private API.
<code>build.source.priority</code>	Приоритет источников данных для фоновой задачи формирования данных об активах.
<code>log.level</code>	Уровень детализации для записи событий, связанных с обращениями к Private API. Возможные значения параметра: <code>debug</code> , <code>info</code> , <code>warning</code> и <code>error</code> . По умолчанию установлен уровень <code>info</code> . Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>api.ksc.insecureskipverify</code>	Если значение параметра <code>True</code> , HTTP-соединение между Private API и Kaspersky Security Center для авторизации выполняется без использования доверенного сертификата.
<code>api.ksc.baseurl</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code>
<code>api.ksc.auth.secretid</code>	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа к Kaspersky Security Center API.
<code>db.driver</code>	Название СУБД, в которой создана база данных решения.
<code>db.host</code>	FQDN или IP-адрес для доступа к устройству с созданной базой данных решения.
<code>db.port</code>	Номер порта для доступа к устройству с созданной базой данных решения.
<code>db.user.file</code>	Путь к файлу с именем роли пользователя для решения в базе данных.
<code>db.pass.file</code>	Путь к файлу с паролем роли пользователя для решения в базе данных.
<code>db.name</code>	Имя базы данных решения.
<code>db.sslmode</code>	Режим SSL для подключения к базе данных решения. Возможные значения: <code>disable</code> , <code>allow</code> , <code>prefer</code> , <code>require</code> , <code>verify-ca</code> , <code>verify-full</code> .
<code>whitebox.public.key.path</code>	Путь к файлу с публичным ключом для задачи <i>Безагентное сканирование в режиме белого ящика</i> .
<code>report.ttl</code>	Время хранения отчетов в часах.
<code>updater.enabled</code>	Параметр включает/выключает обновление баз для модуля анализа соответствия (VMC) и Сетевого сканера. Возможные значения: <code>true</code> или <code>false</code> .
<code>updater.interval</code>	Периодичность обновления баз в часах для модуля анализа соответствия и Сетевого сканера.

publicapi.json

С помощью конфигурационного файла publicapi.json вы можете настраивать параметры службы [Public API](#).

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {  
  "source.priority": ""  
}
```

Параметры конфигурационного файла publicapi.json

Параметр	Описание
<code>http.server.allowedorigins</code>	Определяет, с каких доменов могут быть отправлены запросы к Public API.
<code>http.server.host</code>	URL-адрес сервера, на котором установлен компонент Public API.
<code>http.server.port</code>	Номер порта для доступа к серверу, на котором установлен компонент Public API.
<code>http.server.tls.enable</code>	Параметр определяет использование SSL для подключения к Public API. Возможные значения: <code>true</code> или <code>false</code> .
<code>http.server.tls.servercertfile</code>	Путь к файлу с TLS-сертификатом для доступа к Public API.
<code>http.server.tls.serverkey</code>	Путь к файлу с ключом TLS-сертификата для доступа к Public API.
<code>log.level</code>	Уровень детализации для записи событий, связанных с обращениями к Public API. Возможные значения параметра: <code>debug</code> , <code>info</code> , <code>warning</code> и <code>error</code> . По умолчанию установлен уровень <code>info</code> . Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>api.ksc.insecureskipverify</code>	Если значение параметра <code>True</code> , HTTP-соединение между Public API и Kaspersky Security Center для авторизации выполняется без использования доверенного сертификата.
<code>db.sslmode</code>	Режим SSL для подключения к базе данных решения через Public API. Возможные значения: <code>disable</code> , <code>allow</code> , <code>prefer</code> , <code>require</code> , <code>verify-ca</code> , <code>verify-full</code> .

scanner.json

С помощью конфигурационного файла scanner.json вы можете настраивать параметры [Сетевого сканера](#).

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {  
  "source.priority": ""  
}
```

```
}
```

Параметры конфигурационного файла scanner.json

Параметр	Описание
scan.poller	Блок параметров для получения данных задачи <i>Безагентное сканирование в режиме черного ящика</i> .
job.template	Блок параметров для задачи получения шаблонов nuclei.
log.level	Уровень детализации событий, связанных с работой Сетевого сканера. Возможные значения параметра: debug, info, warning и error. По умолчанию установлен уровень info. Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
taskConfigs	Блок содержит список периодических задач Сетевого сканера и их параметры. Вы можете добавить параметры для задач <i>Безагентное сканирование в режиме белого ящика</i> и <i>Безагентное сканирование в режиме черного ящика</i> и/или удалить имеющиеся параметры.
scan.workerpool.count	Количество параллельных потоков, обрабатывающих задачи Сетевого сканера.
scheduler.sources	Параметр определяет источник задач для сетевого сканера – файл (file) или база данных решения (postgres).
vmapi.client.url	URL-адрес устройства с установленным компонентом Private API.
vmapi.client.insecureskipverify	Если значение параметра True, HTTP-соединение между сетевым сканером и Kaspersky Security Center выполняется без использования доверенного сертификата.
vmapi.client.auth.ksc.url	URL-адрес Сервера администрирования Kaspersky Security Center в формате https://ksc.example.com:13299 для авторизации сетевого сканера перед подключением к Kaspersky Security Center.
vmapi.client.username.file	Путь к файлу с именем служебной учетной записи пользователя для подключения сетевого сканера к Private API.
vmapi.client.password.file	Путь к файлу с паролем служебной учетной записи пользователя для подключения сетевого сканера к Private API.
vmapi.client.auth.secretid	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа сетевого сканера к Private API.
scan.udp.timeout	Тайм-аут ожидания ответа UDP-порта во время выполнения задачи <i>Безагентное сканирование в режиме черного ящика</i> .

updater-compliance.json

С помощью конфигурационного файла updater-compliance.json вы можете настраивать обновление базы уязвимостей для модуля анализа соответствия, которая используется задачей *Сканирование активов на соответствие профилям*.

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра detect.source.priority в конфигурационном файле должно быть записано следующим образом:

```
"detect": {  
  "source.priority": ""  
}
```

Параметр	Описание
<code>app_name</code>	Название решения для загрузки только тех файлов обновлений, которые касаются решения. Должно быть указано <code>VM 1.1. <номер сборки></code>
<code>self_update.enable</code>	Включает или выключает обновление утилиты, с помощью которой выполняется обновление баз уязвимостей. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>true</code> – утилита для обновления баз уязвимостей будет обновляться при наличии обновлений.
<code>type</code>	Задаёт тип источника обновления. Возможные значения: <code>KasperskyLabSecure</code>. Обновления баз поставляются с серверов обновлений "Лаборатории Касперского". <code>LocalTrusted</code>. Обновления баз поставляются из локальной или смонтированной директории на устройстве, задаваемой с помощью дополнительного параметра <code>urls</code>. По умолчанию указано <code>KasperskyLabSecure</code> .
<code>urls</code>	Задаёт директорию с базой уязвимостей, которая будет использоваться для обновления текущей базы уязвимостей. Например: <pre>"urls": "/path/to/update/dir"</pre> Параметр обязателен, если значение параметра <code>type=LocalTrusted</code> .
<code>components</code>	Указывает на компонент решения, для которого обновляются базы уязвимостей. По умолчанию указано <code>VMC</code> – обновляемые базы уязвимостей предназначены для модуля анализа соответствия.
<code>mandatory_components</code>	Указывает на компоненты решения, для которых отсутствие баз уязвимостей прерывает загрузку обновлений для всех указанных с помощью параметра <code>components</code> компонентов решения. Возможные значения: <code>VMD</code>; <code>VMN</code>; <code>VMC</code>. По умолчанию указано <code>VMC</code> .
<code>index</code>	Относительный путь к файлу индексации на сервере обновлений.
<code>updater_files_dir</code>	Директория, в которую сохраняются файлы для обновления утилиты обновления. По умолчанию указана директория <code>/var/lib/kaspersky/vulnerability-management/updater</code> .
<code>download_dir</code>	Директория, в которую сохраняются базы уязвимостей. По умолчанию указана директория <code>/var/lib/kaspersky/vulnerability-management/updater/bases</code> .
<code>update_bases</code>	Включает/выключает обновление базы уязвимостей для модуля анализа соответствия. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>true</code> – база уязвимостей обновляется. Частоту обновления базы уязвимостей для модуля анализа соответствия вы можете настроить с помощью параметра <code>updater.interval</code> в конфигурационном файле <code>privateapi.json</code> .
<code>proxy.enable</code>	Параметр включает/выключает использование прокси-сервера для скачивания баз уязвимостей. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>false</code> – прокси-сервер не используется.
<code>proxy.host</code>	IP-адрес прокси-сервера.
<code>proxy.port</code>	Номер порта прокси-сервера.
<code>proxy.u_path</code>	Название файла, в котором хранится имя учетной записи для аутентификации на прокси-сервере.
<code>proxy.p_path</code>	Название файла, в котором хранится пароль учетной записи для аутентификации на прокси-сервере.

updater-scanner.json

С помощью конфигурационного файла `updater-scanner.json` вы можете настраивать обновление базы уязвимостей для Сетевого сканера, которая используется задачей *Безагентное сканирование в режиме черного ящика*.

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {  
  "source.priority": ""  
}
```

Параметры конфигурационного файла `updater-scanner.json`

Параметр	Описание
<code>app_name</code>	Название решения для загрузки только тех файлов обновлений, которые касаются решения. Должно быть указано <code>VM 1.1.<номер сборки></code>
<code>self_update.enable</code>	Включает или выключает обновление утилиты, с помощью которой выполняется обновление баз уязвимостей. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>true</code> – утилита для обновления баз уязвимостей будет обновляться при наличии обновлений.
<code>type</code>	Задаёт тип источника обновления. Возможные значения: <code>KasperskyLabSecure</code>. Обновления баз поставляются с серверов обновлений "Лаборатории Касперского". <code>LocalTrusted</code>. Обновления баз поставляются из локальной или смонтированной директории на устройстве, задаваемой с помощью дополнительного параметра <code>urls</code>. По умолчанию указано <code>KasperskyLabSecure</code> .
<code>urls</code>	Задаёт директорию с базой уязвимостей, которая будет использоваться для обновления текущей базы уязвимостей. Например: <code>"urls": "/path/to/update/dir"</code> Параметр обязателен, если значение параметра <code>type=LocalTrusted</code> .
<code>components</code>	Указывает на компонент решения, для которого обновляется база уязвимостей. По умолчанию указано <code>VMN</code> – обновляемые базы уязвимостей предназначены для Сетевого сканера.
<code>mandatory_components</code>	Указывает на компоненты решения, для которых отсутствие баз уязвимостей прерывает загрузку обновлений для всех указанных с помощью параметра <code>components</code> компонентов решения. Возможные значения: <code>VMD</code>; <code>VMN</code>; <code>VMC</code>. По умолчанию указано <code>VMN</code> .
<code>index</code>	Относительный путь к файлу индексации на сервере обновлений.
<code>updater_files_dir</code>	Директория, в которую сохраняются файлы для обновления утилиты обновления. По умолчанию указана директория <code>/var/lib/kaspersky/vulnerability-management/updater</code> .
<code>download_dir</code>	Директория, в которую сохраняется база уязвимостей. По умолчанию указана директория <code>/var/lib/kaspersky/vulnerability-management/updater/bases</code> .

Параметр	Описание
<code>update_bases</code>	Включает/выключает обновление базы уязвимостей для Сетевого сканера. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>true</code> – база уязвимостей обновляется. Частоту обновления базы уязвимостей для Сетевого сканера вы можете настроить с помощью параметра <code>updater.interval</code> в конфигурационном файле <code>privateapi.json</code> .
<code>proxy.enable</code>	Включает/выключает использование прокси-сервера для скачивания баз уязвимостей. Возможные значения – <code>true</code> или <code>false</code> . По умолчанию указано значение <code>false</code> – прокси-сервер не используется.
<code>proxy.host</code>	IP-адрес прокси-сервера.
<code>proxy.port</code>	Номер порта прокси-сервера.
<code>proxy.u_path</code>	Название файла, в котором хранится имя учетной записи для аутентификации на прокси-сервере.
<code>proxy.p_path</code>	Название файла, в котором хранится пароль учетной записи для аутентификации на прокси-сервере.

vms.json

С помощью конфигурационного файла `vms.json` вы можете настраивать параметры модуля обнаружения уязвимостей.

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {
  "source.priority":""
}
```

Параметры конфигурационного файла `vms.json`

Параметр	Описание
<code>dump.enable</code>	Включает/выключает создание дампов аварийного завершения работы решения. Возможные значения: <code>true</code> или <code>false</code> . По умолчанию указано значение <code>false</code> – дампы аварийного завершения работы решения не создаются.
<code>dump.dirPath</code>	Задаёт директорию, в которую сохраняются дампы аварийного завершения работы решения. Параметр обязателен, если установлено значение параметра <code>dump.enable=true</code> .
<code>http.certPath</code>	Задаёт путь к сертификату TLS, который необходим для получения данных об уязвимостях.
<code>http.keyPath</code>	Задаёт путь к закрытому ключу TLS.
<code>updater.appFilter</code>	Название решения для загрузки только тех файлов обновлений, которые касаются решения. Должно быть указано <code>VM 1.1.<номер сборки></code>
<code>updater.enable</code>	Включает/выключает обновление базы уязвимостей для модуля обнаружения уязвимостей (VMS). Возможные значения: <code>true</code> или <code>false</code> . По умолчанию указано значение <code>true</code> – обновление баз включено.

Параметр	Описание
<code>type</code>	Задаёт тип источника обновления. Возможные значения: <code>KasperskyLabSecure</code>. Обновления баз поставляются с серверов обновлений "Лаборатории Касперского". <code>LocalTrusted</code>. Обновления баз поставляются из локальной или смонтированной директории на устройстве, задаваемой с помощью дополнительного параметра <code>urls</code>. По умолчанию указано <code>KasperskyLabSecure</code>.
<code>urls</code>	Задаёт директорию с базой уязвимостей, которая будет использоваться для обновления текущей базы уязвимостей. Например: <pre>"urls": "/path/to/update/dir"</pre> Параметр обязателен, если значение параметра <code>type=LocalTrusted</code>.
<code>updater.intervalInHours</code>	Периодичность обновления базы уязвимостей в часах.
<code>updater.updaterFilesDir</code>	Директория, в которую сохраняется база уязвимостей. По умолчанию указана директория <code>/var/lib/kaspersky/vulnerability-management/updater</code>.
<code>updater.target</code>	Идентификатор целевого набора обновлений. Не рекомендуем изменять значение этого параметра. Это может привести к ошибке обновления баз для модуля обнаружения уязвимостей.
<code>updater.useProxy</code>	Включает/выключает использование прокси-сервера для обновления баз уязвимостей. Возможные значения – <code>true</code> или <code>false</code>. По умолчанию указано значение <code>false</code> – прокси-сервер не используется.
<code>ksc.url</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code>
<code>ksc.userPath</code>	Путь к файлу с именем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>ksc.pwdPath</code>	Путь к файлу с паролем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>ksc.caFilePath</code>	Путь к файлу SSL-сертификата для безопасного подключения к Kaspersky Security Center.
<code>ksn.enable</code>	Включает/выключает взаимодействие с KSN. Возможные значения: <code>true</code> или <code>false</code>. По умолчанию указано значение <code>false</code> – взаимодействие с KSN выключено. Параметр используется для включения/выключения взаимодействия с KSN с помощью помощника по настройке. Не рекомендуем изменять значение этого параметра вручную.
<code>ksn.discoveryUrl</code>	URL-адрес сервера KSN в формате <code>https://ksn.example.com:2443</code> .
<code>ksn.acceptedAgreements</code>	В качестве значения параметра может быть указана аббревиатура KSN, означающая, что условия Положения о KSN приняты. Вы можете ознакомиться с условиями Положения о KSN, прочитав текст файла <code>ksn.<идентификатор языка></code>, который включен в комплект поставки решения и расположен после установки компонентов решения в директории <code>/opt/kaspersky/vulnerability-management/doc/</code>. Значение параметра необходимо указывать, если включено взаимодействие с KSN (<code>ksn.enable</code> принимает значение <code>true</code>)
<code>proxy.enable</code>	Включает/выключает использование прокси-сервера для взаимодействия с KSN всеми компонентами решения. Возможные значения – <code>true</code> или <code>false</code>. По умолчанию указано значение <code>false</code> – прокси-сервер не используется.
<code>proxy.host</code>	IP-адрес прокси-сервера.
<code>proxy.port</code>	Номер порта прокси-сервера.

Параметр	Описание
<code>proxy.userPath</code>	Название файла, в котором хранится имя учетной записи для аутентификации на прокси-сервере.
<code>proxy.pwdPath</code>	Название файла, в котором хранится пароль учетной записи для аутентификации на прокси-сервере.

worker.json

Конфигурационный файл `worker.json` содержит параметры [Службы фоновых задач](#).

Не рекомендуем изменять значения параметров, не описанных в таблице ниже. Это может привести к ошибкам в работе Kaspersky Vulnerability Management.

Пути к параметрам необходимо преобразовать в формат JSON. Например, значение параметра `detect.source.priority` в конфигурационном файле должно быть записано следующим образом:

```
"detect": {
  "source.priority": ""
}
```

Параметры конфигурационного файла `worker.json`

Параметр	Описание
<code>ksc.insecureSkipVerify</code>	Параметр в структуре <code>tls.Config</code>, который включает или выключает проверку SSL/TLS-сертификатов сервера. Возможные значения: <code>true</code> или <code>false</code>. Если значение параметра <code>true</code>, HTTP-соединение между службой фоновых задач (Worker) и Kaspersky Security Center для импорта данных об активах выполняется без использования доверенного сертификата.
<code>worker.ksc.username.file</code>	Путь к файлу с именем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>worker.ksc.password.file</code>	Путь к файлу с паролем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>kscsync.enabled</code>	Параметр включает/выключает синхронизацию задач Kaspersky Security Center и Kaspersky Vulnerability Management. Возможные значения: <code>true</code> или <code>false</code>. Если значение параметра <code>true</code> синхронизация задач включена.
<code>kscsync.ksc.insecureskipverify</code>	Параметр в структуре <code>tls.Config</code>, который включает или выключает проверку SSL/TLS-сертификатов сервера. Возможные значения: <code>true</code> или <code>false</code>. Если значение параметра <code>true</code>, HTTP-соединение между службой фоновых задач (Worker) и Kaspersky Security Center для синхронизации задач выполняется без использования доверенного сертификата.
<code>kscsync.ksc.auth.secretid</code>	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа к Kaspersky Security Center. Не рекомендуем менять это значение, так как это может привести к нарушению синхронизации задач между Kaspersky Vulnerability Management и Сервером администрирования.
<code>kscsync.ksc.baseurl</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code> .

Параметр	Описание
<code>vmdclient.insecureskipverify</code>	Параметр в структуре <code>tls.Config</code> , который включает или выключает проверку SSL/TLS-сертификатов сервера. Возможные значения: <code>true</code> или <code>false</code> . Если значение параметра <code>true</code> , HTTP-соединение между службами Worker и VMS выполняется без использования доверенного сертификата.
<code>vmdclient.auth.secretid</code>	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа к Kaspersky Security Center.
<code>vmdclient.auth.ksc.url</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code> для авторизации службы фоновых задач перед подключением к Kaspersky Security Center.
<code>vmdclient.baseurl</code>	URL-адрес устройства, на котором установлен компонент VMS.
<code>vmdclient.username.file</code>	Путь к файлу с именем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>vmdclient.password.file</code>	Путь к файлу с паролем учетной записи пользователя для подключения к Kaspersky Security Center.
<code>taskConfigs</code>	Блок содержит параметры фоновых и системных задач.
<code>detect.source.priority</code>	Параметр определяет приоритет источника найденных уязвимостей. Имеет значение на этапе обработки данных об уязвимостях, если выполнялись задачи <i>Поиск уязвимостей</i> (<code>"agent": 0</code>), <i>Безагентное сканирование в режиме черного ящика</i> (<code>"blackbox": 1</code>) и <i>Безагентное сканирование в режиме белого ящика</i> (<code>"whitebox": 2</code>).
<code>detect.write.worker.count</code>	Количество параллельных процессов для сохранения данных об уязвимостях. Рекомендуемое значение – 10.
<code>software.inventory.source.priority</code>	Приоритет источника данных о программном обеспечении, который учитывается в процессе слияния данных: результаты выполнения задачи <i>Поиск уязвимостей</i> (<code>"agent": 0</code>) или <i>Безагентное сканирование в режиме белого ящика</i> (<code>"whitebox": 2</code>).
<code>build.source.priority</code>	Приоритет источников данных для фоновой задачи формирования данных об активах.
<code>compliance.ksc.insecureSkipVerify</code>	Параметр в структуре <code>tls.Config</code> , который включает или выключает проверку SSL/TLS-сертификатов сервера. Возможные значения: <code>true</code> или <code>false</code> . Если значение параметра <code>true</code> , HTTP-соединение между службой фоновых задач (Worker) и Kaspersky Security Center для выполнения задачи <i>Сканирование активов на соответствие профилям</i> выполняется без использования доверенного сертификата.
<code>compliance.ksc.auth.secretid</code>	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа к Kaspersky Security Center.
<code>compliance.ksc.baseurl</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code> для авторизации модуля анализа соответствия перед подключением к Kaspersky Security Center.
<code>compliance.unsqueeze.updateable.bases</code>	Параметр указывает, нужно ли перед отправкой Агенту администрирования выполнять декомпрессию баз для модуля анализа соответствия (VMC). Возможные значения: <code>true</code> или <code>false</code> .
<code>vmd.detect.asset.cache.chunk.size</code>	Размер пакета активов, SBOM которых сканируется на уязвимости, в мегабайтах. Значение по умолчанию равно 50 мегабайтам. Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>vmd.detect.scan.chunk.size</code>	Размер пакета SBOM для сканирования в мегабайтах. Значение по умолчанию равно ста мегабайтам. Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>vmd.detect.s bom.read.worker.count</code>	Количество параллельных процессов для получения SBOM для сканирования.
<code>vmd.detect.save.worker.count</code>	Количество параллельных процессов для сохранения данных об уязвимостях.
<code>scheduler.config.refresh.interval</code>	Периодичность применения обновлений конфигурационного файла в минутах. Значение по умолчанию равно одной минуте. Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>scheduler.taskconfig.sources</code>	Источник данных о задачах решения. Возможные значения: база данных решения (postgres) или файл (file).

Параметр	Описание
<code>log.level</code>	Уровень детализации событий, связанных с фоновыми и системными задачами. Возможные значения параметра: <code>debug</code> , <code>info</code> , <code>warning</code> и <code>error</code> . По умолчанию установлен уровень <code>info</code> . Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>log.writer.file.maxagedays</code>	Срок хранения журнала событий фоновых и системных задач. Значение по умолчанию равно 30 дням. Вы можете добавить этот параметр в конфигурационный файл для изменения значения по умолчанию.
<code>whitebox.private.key.path</code>	Путь к приватному ключу с именем <code>whitebox.key</code> для задачи <i>Безагентное сканирование в режиме белого ящика</i> .
<code>tracing.enabled</code>	Параметр включает/выключает трассировку работы службы фоновых задач (Worker). Возможные значения: <code>true</code> или <code>false</code> .
<code>vmapi.client.url</code>	URL-адрес сервера, на котором установлен компонент Private API.
<code>vmapi.client.insecureskipverify</code>	Параметр в структуре <code>tls.Config</code> , который включает или выключает проверку SSL/TLS-сертификатов сервера. Возможные значения: <code>true</code> или <code>false</code> . Если значение параметра <code>true</code> , HTTP-соединение с сервером, на котором установлен компонент Private API, выполняется без использования доверенного сертификата.
<code>vmapi.client.auth.ksc.url</code>	URL-адрес Сервера администрирования Kaspersky Security Center в формате <code>https://ksc.example.com:13299</code> .
<code>vmapi.client.username.file</code>	Путь к файлу с именем учетной записи пользователя для подключения службы фоновых задач к Private API.
<code>vmapi.client.password.file</code>	Путь к файлу с паролем учетной записи пользователя для подключения службы фоновых задач к Private API.
<code>vmapi.client.auth.secretid</code>	Префикс, в котором отображается путь до параметров секретов, которые используются для доступа службы фоновых задач к Private API.
<code>db.driver</code>	Название СУБД, в которой создана база данных решения.
<code>db.host</code>	FQDN или IP-адрес для доступа к устройству с созданной базой данных решения.
<code>db.port</code>	Номер порта для доступа к созданной базе данных решения.
<code>db.user.file</code>	Путь к файлу с именем роли пользователя для решения в базе данных.
<code>db.pass.file</code>	Путь к файлу с паролем роли пользователя для решения в базе данных.
<code>db.name</code>	Имя базы данных решения.
<code>db.sslmode</code>	Режим SSL для подключения к базе данных решения. Возможные значения: <code>disable</code> , <code>allow</code> , <code>prefer</code> , <code>require</code> , <code>verify-ca</code> , <code>verify-full</code> .
<code>ssh.connect.timeout</code>	Максимальное время ожидания подключения по SSH к активу для сканирования в режиме белого ящика. Если SSH-соединение не устанавливается за это время, попытка считается неудачной и завершается ошибкой. По умолчанию указано значение 30 секунд
<code>ssh.read.timeout</code>	Максимальное время ожидания данных от актива после SSH-подключения. Если за это время данные от актива не поступают, попытка считается неудачной и завершается ошибкой. По умолчанию указано значение 30 секунд.
<code>ssh.write.timeout</code>	Максимальное время ожидания отправки данных по SSH на актив для сканирования в режиме белого ящика. Если данные не удастся отправить за заданное время, операция записи завершается ошибкой. По умолчанию указано значение 30 секунд
<code>locales</code>	Задаёт языки, на которых описания уязвимостей хранятся в базе данных решения. По умолчанию указано * – описания уязвимостей хранятся в базе данных решения на всех доступных языках.

Параметр	Описание
<code>import.workersCount</code>	Максимальное количество процессов службы фоновых задач, которые одновременно импортируют данные об активах из Kaspersky Security Center в базу данных решения.
<code>import.write.batch.size</code>	Максимальное количество активов, данные о которых сохраняются в базе данных решения одним пакетом при импорте из Kaspersky Security Center

Использование помощника по настройке

Для настройки решения и выполнения некоторых вспомогательных команд вы можете запускать помощника по настройке:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh
[configure|unattendedconfigure|start|stop|restart|status|collect-logs|ksn-
participating|setplugin|updatemode|rotate-certs|help]
```

Где:

- `configure`. Помощник по настройке запускается в интерактивном режиме для полной настройки решения.
- `unattendedconfigure`. Помощник по настройке запускается в тихом режиме для полной настройки решения. Вместе с этим параметром требуется добавить `KVMANSWERSFILE=/path/to/file.json`, где `/path/to/file.json` – путь к JSON-файлу с параметрами для настройки Kaspersky Vulnerability Management.

```
{
  "eulaAccepted":true,
  "privacyPolicyAccepted":true,
  "ksnAgreementAccepted":true|false,
  "database":
  {
    "host":"",
    "port":,
    "dbname":"",
    "dbschema":"",
    "dbuser":"",
    "dbpassword":"",
    "dbssl":
    {
      "mode":"verify-full|disable|allow|prefer|require|verify-ca",
      "certpath":""
    }
  },
  "proxy":
  {
    "enabled":true|false,
    "host":"",
    "port":,
    "login":"",
    "password":""
  },
  "ksc":
  {
    "apiurl":"",
    "iamproxyurl":"",
    "users":
    {
      "worker":
      {
        "username":"",
        "password":""
      },
      "scanner":

```

```

        {
            "username": "",
            "password": ""
        }
    },
    "tls": {
        "certificates": "generate|existing",
        "existing": {
            "type": "ca|selfsigned",
            "services": {
                "ca": {
                    "certpath": ""
                },
                "privateapi": {
                    "certpath": "",
                    "keypath": ""
                },
                "publicapi": {
                    "certpath": "",
                    "keypath": ""
                },
                "vms": {
                    "certpath": "",
                    "keypath": ""
                }
            }
        }
    }
}

```

Параметры файла `file.json` определяют следующее:

`.eulaAccepted` (boolean) — признак согласия с Лицензионным соглашением. Для продолжения настройки должен быть `true`.

`.privacyPolicyAccepted` (boolean) — признак согласия с "Политикой конфиденциальности". Для продолжения настройки должен быть `true`.

`.ksnAgreementAccepted` (boolean) — признак принятия Положения о KSN, влияет на работу модуля обнаружения уязвимостей. Возможные значения: `true` или `false`.

Функциональность KSN может быть недоступна в решении на территории США.

`.database.host` (string) — FQDN или IP-адрес для доступа к устройству с созданной базой данных решения.

`.database.port` (int) — номер порта для доступа к устройству с созданной базой данных решения.

`.database.dbname` (string) — имя базы данных решения.

`.database.dbschema` (string) — схема в базе данных, с которой будет работать решение.

`.database.dbuser` (string) — имя роли пользователя для решения в базе данных.

`.database.dbpassword` (string) — пароль роли пользователя для решения в базе данных.

`.database.dbssl.mode` (string) — режим SSL для подключения к базе данных. Возможные значения: `verify-full|disable|allow|prefer|require|verify-ca`. Подробнее о каждом режиме см. в [документации к PostgreSQL](#).

`.database.dbssl.certpath` (string) — путь к SSL-сертификату базы данных. Обязателен, если для параметра `.database.dbssl.mode` указано одно из значений `verify-full|require|verify-ca`.

`.proxy.enabled` (boolean) — признак, определяющий необходимость использовать прокси-сервер для доступа к [обновляемым базам](#). Если значение равно `true`, то все остальные значения раздела `.proxy` должны быть указаны. Значения этих параметров вы можете посмотреть в Kaspersky Security Center Web Console в разделе **Параметры** → **Интеграция** на вкладке **Параметры прокси-сервера Web Console**.

`.proxy.host` (string) — адрес прокси-сервера в формате `proxy.example.com`.

`.proxy.port` (int) — порт прокси-сервера (по умолчанию — 8080).

`.proxy.login` (string) — имя пользователя для аутентификации на прокси-сервере. Для анонимной аутентификации на прокси-сервере не указывайте значение.

`.proxy.password` (string) — пароль пользователя для аутентификации на прокси-сервере. Для анонимной аутентификации на прокси-сервере не указывайте значение.

`.ksc.apiurl` (string) — адрес для доступа к Kaspersky Security Center API в формате `https://ksc.example.com:13299`.

`.ksc.iamproxyurl` (string) — адрес для доступа к Kaspersky Security Center IAM Proxy в формате `https://ksc-iam.example.com:9050`.

`.ksc.users.worker.username` (string) — имя учетной записи VM Worker, [созданной перед установкой компонентов Kaspersky Vulnerability Management](#).

`.ksc.users.worker.password` (string) — пароль учетной записи VM Worker.

`.ksc.users.scanner.username` (string) — имя учетной записи VM Scanner с ролью VM Scanner, созданной перед установкой компонентов Kaspersky Vulnerability Management.

`.ksc.users.scanner.password` (string) — пароль учетной записи VM Scanner.

`.tls.certificates` (string) — способ указания TLS-сертификатов. Возможные значения:

- `generate`. Если указано это значение, помощник по настройке самостоятельно создает TLS-сертификаты, заполнять остальные поля в блоке `.tls` не требуется.
- `existing`. Если указано это значение, необходимо ввести пути к заранее созданным TLS-сертификатам и заполнить остальные поля в блоке `.tls`.

`.tls.existing.type` (string) — тип заранее созданных TLS-сертификатов. Возможные значения:

- `ca`. Сертификаты выписаны корпоративным центром сертификации. Все сертификаты должны быть выписаны одними и теми же корневым и промежуточным (если такой используется в организации) центрами сертификации.
- `selfsigned`. Самоподписанные сертификаты.

`.tls.existing.services.ca.certpath` (string) — путь к файлу с цепочкой сертификатов корпоративного центра сертификации. Должен содержать сертификаты как корневого, так и промежуточного (если используется в организации) центров сертификации. Поле не требуется заполнять, если `.tls.existing.type` имеет значение `selfsigned`.

`.tls.existing.services.privateapi.certpath` (string) — путь к файлу с сертификатом для Private API. Файл должен быть незашифрованным.

`.tls.existing.services.privateapi.keypath` (string) — путь к файлу с ключом сертификата для Private API. Файл должен быть незашифрованным.

`.tls.existing.services.publicapi.certpath` (string) — путь к файлу с сертификатом для Public API. Файл должен быть незашифрованным.

`.tls.existing.services.publicapi.keypath` (string) — путь к файлу с ключом сертификата для Public API. Файл должен быть незашифрованным.

`.tls.existing.services.vms.certpath` (string) — путь к файлу с сертификатом для VMS. Файл должен быть незашифрованным.

`.tls.existing.services.vms.keypath` (string) — Путь к файлу с ключом сертификата для VMS. Файл должен быть незашифрованным.

Например: `sudo KVMANSWERSFILE=/path/to/file.json /opt/kaspersky/vulnerability-management/helper/helper.sh unattendedconfigure`

- `start`. Помощник по настройке запускает процессы компонентов решения.
- `stop`. Помощник по настройке останавливает процессы компонентов решения.
- `restart`. Помощник по настройке останавливает и далее запускает процессы компонентов решения.
- `status`. Помощник по настройке выводит статус работы компонентов решения.
- `collect-logs`. Помощник по настройке собирает [журналы событий](#) и доступные для редактирования [конфигурационные файлы](#), помещает их в архив и выводит путь к архиву.
- `ksn-participating`. Помощник по настройке предоставляет возможность изменить решение о принятии условий Положения о KSN. Если вы принимаете условия Положения о KSN, взаимодействие с KSN включается. Если вы не принимаете условия Положения о KSN, взаимодействие с KSN выключается.
Вы можете ознакомиться с условиями Положения о KSN, прочитав текст файла `ksn.<идентификатор языка>`, который включен в [комплект поставки решения](#) и расположен после установки компонентов решения в директории `/opt/kaspersky/vulnerability-management/doc/`.
- `setplugin`. Помощник по настройке устанавливает и настраивает хранилище данных плагинов в Kaspersky Security Center. Может понадобиться, если необходимо заменить сертификат Private API, изменить адрес устройства для установки Private API или если во время установки не удалось установить или проверить хранилище данных плагинов.
- `updatemode`. Помощник по настройке предоставляет возможность изменить источник для обновления баз уязвимостей.

- `rotate-certs`. Помощник по настройке выполняет следующие действия:
 - Выпускает новые сертификаты для служб Private API, Public API и VMS.
 - Обновляет сертификаты KSC OpenAPI и IAM для доверия им со стороны служб Kaspersky Vulnerability Management.
 - Прописывает новый сертификат Private API в хранилище данных плагинов в Kaspersky Security Center.
- `help`. Вызов справки со списком всех доступных параметров и их описаниями.

Например:

```
sudo /opt/kaspersky/vulnerability-management/helper/helper.sh updatemode
```

Разделение доступа к функциям решения по пользовательским ролям

Доступ пользователей к функциям и данным Kaspersky Vulnerability Management разделяется с помощью ролей. Роль определяет, какие действия пользователь может выполнять в функциональных областях решения: например, просматривать активы, запускать поиск уязвимостей, импортировать профили соответствия или формировать отчеты.

Общие принципы разграничения доступа

Разграничение доступа основано на функциональных областях Kaspersky Vulnerability Management. Для каждой функциональной области настраивается набор прав доступа.

Права доступа для функциональных областей могут быть заданы одним из следующих способов:

- *Разрешить* — пользователь может выполнять соответствующее действие.
- *Запретить* — пользователь не может выполнять соответствующее действие.
- *Не определено* — право не задано; соответствующее действие недоступно.

Если для одной и той же функциональной области в разных ролях есть конфликт прав доступа, приоритет имеет явный запрет. Например, если одна роль разрешает просмотр активов, а другая роль запрещает его, пользователь с этими ролями не сможет просматривать активы.

Изменения прав для пользователей с активной сессией могут применяться с задержкой до пяти минут.

Функциональные области Kaspersky Vulnerability Management

После установки веб-плагина управления решением в списке прав доступа Kaspersky Security Center появляются функциональные области Kaspersky Vulnerability Management.

Вы можете создавать роли с произвольным набором прав для следующих функциональных областей решения.

Права доступа к функциональным областям Kaspersky Vulnerability Management

Функциональная область	Право доступа	Что дает право доступа
Активы Управляет доступом к сведениям об активах ИТ-инфраструктуры организации.	Чтение	Просмотр и экспорт информации об активах, установленном программном обеспечении, найденных уязвимостях, открытых сетевых портах и доступных через них сервисах, результатах сканирования на соответствие профилям.
	Запись	Изменение значимости активов.
Группы активов	Чтение	Просмотр информации о группах активов.
	Запись	Добавление и удаление групп активов.
Анализ соответствия Управляет доступом к профилям соответствия и результатам проверок.	Чтение	Просмотр профилей соответствия, правил профилей, результатов проверок и получение ссылок для загрузки результатов.
	Запись	Удаление и импорт профилей соответствия.
Сетевое сканирование API Управляет доступом к API Сетевого сканера. Предназначена для служебных компонентов решения, а не для пользователей.	Чтение	Просмотр шаблонов Nuclei, используемых Сетевым сканером.
	Запись	Удаление задач сетевого сканирования из очереди, добавление результатов сетевого сканирования в базу данных решения.
Публичный API: - Активы - Уязвимости - Программное обеспечение Предоставляет возможность сторонним системам получать данные об активах и найденных уязвимостях.	Чтение	Получение через Public API списка активов, уязвимостей на активах, данных о программном обеспечении, установленном на активах.
Отчеты Управляет доступом к просмотру и работе с отчетами.	Чтение	Просмотр шаблонов отчетов и отчетов, экспорт отчетов.
	Запись	Создание, изменение и удаление шаблонов отчетов, удаление отчетов.
	Выполнение	Запуск и остановка генерации отчетов.
Программное обеспечение Управляет доступом к сведениям об установленном программном обеспечении.	Чтение	Просмотр сведений об установленном программном обеспечении, связанных с ним уязвимостях и активах, на которых установлено программное обеспечение. Получение SBOM для активов через соответствующий метод Kaspersky Security Center OpenAPI.
Уязвимости Управляет доступом к данным об уязвимостях.	Чтение	Просмотр и экспорт информации об уязвимостях, затронутых активах и программном обеспечении.
	Выполнение	Запуск задач сканирования, формирование обнаружений и получение сведений об уязвимостях по их идентификаторам.

Примеры пользовательских ролей

Аналитик уязвимостей

Эта роль предназначена для пользователя, который анализирует уже найденные уязвимости, оценивает их влияние и готовит выводы для ИБ- или ИТ-команд.

Для аналитика уязвимостей рекомендуем следующие права:

- Уязвимости — чтение, чтобы видеть результаты поиска уязвимостей.
- Активы — чтение и Программное обеспечение — чтение нужны для контекста: аналитику уязвимостей важно понимать, на каких активах выполняются задачи сканирования и какое программное обеспечение связано с результатами сканирования.
- Отчеты — чтение, чтобы просматривать сгенерированные отчеты.

Оператор сканирования

Эта роль предназначена для пользователя, который выполняет действия, связанные с поиском и анализом уязвимостей.

Для оператора сканирования рекомендуем следующие права:

- Уязвимости — чтение, чтобы видеть результаты поиска уязвимостей.
- Уязвимости — выполнение, чтобы запускать задачи сканирования.
- Активы — чтение и Программное обеспечение — чтение нужны для контекста: оператору сканирования важно понимать, на каких активах выполняются задачи сканирования и какое программное обеспечение связано с результатами сканирования.

Аудитор соответствия

Эта роль предназначена для пользователя, который анализирует активы на соответствие профилям.

Для аудитора соответствия рекомендуем следующие права:

- Анализ соответствия — чтение, чтобы просматривать профили соответствия и результаты сканирования на соответствие профилям.
- Активы — чтение, понимать, к каким активам относятся результаты.
- Отчеты — чтение, чтобы просматривать сгенерированные отчеты.

Создание пользовательских профилей соответствия

В этом разделе описаны требования к подготовке ZIP-архива с профилями соответствия для [импорта в Kaspersky Vulnerability Management](#).

ZIP-архив должен содержать связанные между собой XCCDF-файл и OVAL-файлы.

XCCDF-файл описывает бенчмарк, профили соответствия, правила и состав проверок, входящих в профили соответствия. OVAL-файлы описывают техническую логику проверок, на которые ссылаются правила из XCCDF-файла.

Для корректного импорта рекомендуем использовать следующую структуру ZIP-архива с профилями соответствия:

```
profile(s).zip
├── xccdf.xml
├── checks-1-oval.xml
├── checks-2-oval.xml
├── ...
└── checks-n-oval.xml
```

При этом должны быть выполнены следующие требования:

- архив должен содержать один XCCDF-файл;
- архив должен содержать один или несколько OVAL-файлов;
- XCCDF- и OVAL-файлы должны находиться в корне архива.

Импорт профилей соответствия, описанных в файле формата SCAP DataStream, не поддерживается.

Требования к XCCDF-файлу

XCCDF-файл должен содержать один корневой элемент `Benchmark`. В элементе нем должны быть описаны:

- идентификатор бенчмарка в атрибуте `Benchmark/@id`, например: `id="xccdf_custom_benchmark_windows"`;
- язык содержимого в атрибуте `Benchmark/@xml:lang`, например: `xml:lang="en-US"`;
- статус бенчмарка в элементе `Benchmark/status`, например: `<status>accepted</status>`;
- название бенчмарка в элементе `Benchmark/title`, например: `<title xml:lang="ru-RU">Проверки конфигурации ОС Windows на соответствие требованиям нормативных, методических и организационных документов</title>`;
- описание бенчмарка в элементе `Benchmark/description`, например: `<description xml:lang="ru-RU">Бенчмарк содержит набор профилей для оценки соответствия конфигурации ОС Windows требованиям нормативных, методических и организационных документов...</description>`;
- версия бенчмарка в элементе `Benchmark/version`, например: `<version>1.0</version>`;
- один или несколько профилей соответствия в элементах `Benchmark/Profile`, например: `<Profile id="xccdf_custom_profile_standard">`;
- правила в элементах `Benchmark/Rule`, например: `<Rule id="xccdf_custom_rule_1" selected="false">`;
- ссылки из правил на OVAL-проверки через элементы `Rule/check` и `Rule/check/check-content-ref`, например: `<check-content-ref href="checks-oval.xml" name="oval:custom:def:20000001"/>`.

Один бенчмарк может содержать несколько профилей соответствия. Каждый профиль соответствия должен явно указывать состав входящих в него правил через элементы `select`.

Идентификаторы элементов должны быть уникальными и стабильными в рамках импортируемого комплекта файлов. Допускается использование собственной схемы именования идентификаторов, если между элементами сохранены корректные связи:

- `Profile/select/@idref` должен ссылаться на существующий `Rule/@id`;
- `Rule/check/check-content-ref/@href` должен указывать на OVAL-файл, находящийся в корне ZIP-архива;
- `Rule/check/check-content-ref/@name` должен указывать на существующий `definition/@id` внутри указанного OVAL-файла.

Рекомендуем использовать единообразную и понятную схему именования идентификаторов.

Пример содержимого XCCDF-файла

```
<Benchmark id="xccdf_custom_benchmark_ubuntu" ...>
  <status>accepted</status>
  <title>Проверки конфигурации ОС Ubuntu</title>
  <description>Описание бенчмарка</description>
  <version>1.0</version>
  <Profile id="xccdf_custom_profile_id">
    <title>Профиль ФСТЭК России №21 для ОС Ubuntu</title>
    <description>Описание профиля</description>
    <select idref="xccdf_custom_rule_1" selected="true"/>
    <select idref="xccdf_custom_rule_2" selected="true"/>
  </Profile>
  <Rule id="xccdf_custom_rule_1" selected="false">
    <title>Название правила</title>
    <description>Описание правила</description>
    <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-content-ref href="checks-oval.xml" name="oval:custom:def:1"/>
    </check>
  </Rule>
</Benchmark>
```

В примере имена идентификаторов приведены условно. Вы можете использовать другую схему именования, если идентификаторы уникальны и корректно связаны между собой.

Требования к профилям

Каждый профиль должен быть описан элементом `Profile`.

Профиль должен содержать:

- уникальный идентификатор в атрибуте `Profile/@id`, например: `id="xccdf_custom_profile_standard"`;
- название профиля в элементе `Profile/title`, например: `<title xml:lang="ru-RU">Профиль ФСТЭК России №21 для ОС Windows</title>`;
- описание профиля в элементе `Profile/description`, например: `<description xml:lang="ru-RU">Профиль включает в себя проверки конфигурационных параметров ОС Windows...</description>`;
- ссылку на документ-основание в элементе `Profile/reference`, если она используется, например: `<reference>https://fstec.ru/...</reference>`;

- список выбранных правил в элементах Profile/select, например: `<select idref="xccdf_custom_rule_1" selected="true"/>`;
- ссылку на правило в атрибуте Profile/select/@idref, например: `idref="xccdf_custom_rule_1"`;
- признак включения правила в профиль в атрибуте Profile/select/@selected, например: `selected="true"`.

Элемент `select` должен ссылаться на существующее правило по его идентификатору Rule/@id.

Пример:

```
<Profile id="xccdf_example_profile">
  <title>Профиль проверки конфигурации</title>
  <description>Описание профиля</description>
  <select idref="xccdf_example_rule_1" selected="true"/>
</Profile>
```

Требования к правилам

Каждое правило должно быть описано элементом Rule.

Правило должно содержать:

- уникальный идентификатор в атрибуте Rule/@id, например: `id="xccdf_custom_rule_1"`;
- признак выбора правила по умолчанию в атрибуте Rule/@selected, например: `selected="false"`;
- название правила в элементе Rule/title, например: `<title xml:lang="ru-RU">Принудительное использование истории паролей</title>`;
- описание правила в элементе Rule/description, например: `<description xml:lang="ru-RU">Необходимо убедиться, что система хранит историю ранее использованных паролей...</description>`;
- идентификаторы требований в элементах Rule/ident, например: `<ident system="xccdf_custom_profile_standard">ИАФ.4</ident>`;
- систему идентификаторов требований в атрибуте Rule/ident/@system, например: `system="xccdf_custom_profile_standard"`;
- ссылку на OVAL-файл в атрибуте Rule/check/check-content-ref/@href, например: `href="checks-oval.xml"`;
- ссылку на OVAL definition в атрибуте Rule/check/check-content-ref/@name, например: `name="oval:custom:def:20000001"`.

Пример:

```
<Rule id="xccdf_example_rule_1" selected="false">
  <title>Название правила</title>
  <description>Описание правила</description>
  <ident system="custom_requirements">REQ.1</ident>
```

```
<check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
  <check-content-ref href="checks-oval.xml" name="oval:example:def:1"/>
</check>
</Rule>
```

Значение href должно указывать на OVAL-файл, который находится в том же ZIP-архиве в корне архива.

Значение name должно указывать на существующий OVAL definition/@id внутри указанного OVAL-файла.

Требования к OVAL-файлам

OVAL-файл должен быть корректным XML-документом с корневым элементом oval_definitions.

В OVAL-файле могут быть описаны:

- сведения о генераторе в элементе oval_definitions/generator, например: <generator>...</generator>;
- название продукта в элементе generator/oval:product_name, например: <oval:product_name>Название</oval:product_name>;
- версия OVAL-схемы в элементе generator/oval:schema_version, например: <oval:schema_version>5.11.2</oval:schema_version>;
- время формирования файла в элементе generator/oval:timestamp, например: <oval:timestamp>2026-01-01T00:00:00Z</oval:timestamp>;
- версия продукта в элементе generator/oval:product_version, например: <oval:product_version>1.1</oval:product_version>;
- список OVAL-проверок в элементе oval_definitions/definitions, например: <definitions>...</definitions>;
- конкретная OVAL-проверка в блоке definitions/definition, например: <definition id="oval:custom:def:1" version="1" class="compliance">. В блоке definition могут быть описаны:
 - уникальный идентификатор в атрибуте definition/@id, например: id="oval:custom:def:1";
 - версия в атрибуте definition/@version, например: version="1";
 - класс проверки в атрибуте definition/@class, например: class="compliance";
 - метаданные проверки в блоке definition/metadata, например: <metadata>...</metadata>. В блоке metadata могут быть описаны:
 - название OVAL-проверки в элементе metadata/title, например: <title>Принудительное использование истории паролей</title>;
 - описание OVAL-проверки в элементе metadata/description, например: <description>Проверяется, что значение параметра password_hist_len больше или равно 24</description>;
 - применимая платформа в элементе metadata/affected, например: <affected family="windows">...</affected>;

- семейство платформы в атрибуте `metadata/affected/@family`, например: `family="windows"`;
- конкретные платформы в элементах `metadata/affected/platform`, например:
`<platform>Windows 10</platform>`.
- критерии проверки в блоке `definition/criteria`, например: `<criteria>...</criteria>`. В блоке `criteria` могут быть описаны:
 - условия проверки в элементах `definition/criteria/criterion`, например: `<criterion test_ref="oval:custom:tst:1" comment="Описание условия проверки"/>`;
 - внешние ссылки на OVAL-определения внутри того же бенчмарка с помощью элементов `definition/criteria/extend_definition`, например: `<extend_definition definition_ref="oval:custom:def:10" version="1" class="compliance" comment="Комментарий"/>`.

Внешние ссылки на OVAL-определения из архива другого бенчмарка не поддерживаются. Такой бенчмарк возможно импортировать, но сканирование активов на соответствие его профилям завершится с ошибкой.

- используемые тесты в элементе `oval_definitions/tests`, например: `<tests>...</tests>`;
- конкретный тест в элементе `tests/windows:passwordpolicy_test`, например:
`<windows:passwordpolicy_test id="oval:custom:tst:1" version="1" check="all">`;
- используемые объекты в элементе `oval_definitions/objects`, например: `<objects>...</objects>`;
- конкретный объект в элементе `objects/windows:passwordpolicy_object`, например:
`<windows:passwordpolicy_object id="oval:custom:obj:1" version="1"/>`;
- используемые состояния в элементе `oval_definitions/states`, если они требуются проверками, например: `<states>...</states>`;
- конкретное состояние в элементе `states/windows:passwordpolicy_state`, например:
`<windows:passwordpolicy_state id="oval:custom:ste:1" version="1">`;
- используемые переменные в элементе `oval_definitions/variables`, если они требуются проверками, например: `<variables>...</variables>`;
- конкретная переменная в элементе `variables/constant_variable`, например: `<constant_variable id="oval:custom:var:1" version="1" datatype="int">`.

Пример блока `definition`

```
<definition id="oval:custom:def:1" version="1" class="compliance">
  <metadata>
    <title>Принудительное использование истории паролей</title>
    <description>Проверяется, что значение параметра password_hist_len больше или равно 24.</description>
    <affected family="windows">
      <platform>Windows 10</platform>
      <platform>Windows 11</platform>
      <platform>Windows Server 2019</platform>
      <platform>Windows Server 2022</platform>
    </affected>
  </metadata>
  <criteria>
    <criterion test_ref="oval:custom:tst:1" comment="Проверка значения password_hist_len"/>
  </criteria>
</definition>
```

```
</criteria>  
</definition>
```

Требования к идентификаторам OVAL

Все элементы OVAL, на которые выполняются ссылки, должны иметь уникальные идентификаторы.

Идентификаторы OVAL должны использовать стандартный формат: `oval:<namespace>:<type>:<number>`

Где:

- `<namespace>` – пространство имен поставщика или профиля;
- `<type>` – тип OVAL-элемента;
- `<number>` – числовой идентификатор элемента.

Допустимые значения `<type>`:

- `def` – definition;
- `tst` – test;
- `obj` – object;
- `ste` – state;
- `var` – variable.

Примеры идентификаторов:

```
oval:custom:def:1  
oval:custom:tst:1  
oval:custom:obj:1  
oval:custom:ste:1  
oval:custom:var:1
```

Допускается использовать собственное пространство имен, например:

```
oval:example.company.security:def:10000001  
oval:example.company.security:tst:10000001  
oval:example.company.security:obj:10000001  
oval:example.company.security:ste:10000001
```

Идентификаторы должны быть стабильными и не должны изменяться между версиями одного и того же профиля соответствия без необходимости.

Поддерживаемые типы OVAL-тестов

В пользовательских OVAL-файлах допускается использование следующих типов тестов:

- Проверки Linux:

```
ind:textfilecontent54_test
ind:variable_test
linux:inetlisteningserver_test
linux:partition_test
linux:systemdunitproperty_test
unix:file_test
unix:password_test
unix:sysctl_test
```

- Проверки DEB-пакетов (для Debian, Ubuntu, Astra Linux и других DEB-based систем):

```
linux:dpkginfo_test
```

- Проверки RPM-пакетов (для ALT Linux, RedOS и других RPM-based систем):

```
linux:rpminfo_test
```

- Проверки Windows:

```
windows:auditeventpolicysubcategories_test
windows:lockoutpolicy_test
windows:passwordpolicy_test
windows:registry_test
windows:sid_sid_test
windows:user_sid55_test
windows:userright_test
windows:wmi57_test
```

Использование других типов OVAL-тестов не поддерживается.

Требования к tests, objects и states

Каждый OVAL-тест должен ссылаться на существующий объект через элемент `object_ref`.

Если для проверки требуется сравнение с ожидаемым значением, тест должен ссылаться на существующее состояние через элемент `state_ref`.

Типы `test`, `object` и `state` должны соответствовать друг другу.

Пример:

```
<tests>
  <ind:textfilecontent54_test id="oval:custom:tst:1" version="1" check="all">
    <ind:object object_ref="oval:custom:obj:1"/>
    <ind:state state_ref="oval:custom:ste:1"/>
  </ind:textfilecontent54_test>
```

```

</tests>
<objects>
  <ind:textfilecontent54_object id="oval:custom:obj:1" version="1">
    ...
  </ind:textfilecontent54_object>
</objects>
<states>
  <ind:textfilecontent54_state id="oval:custom:ste:1" version="1">
    ...
  </ind:textfilecontent54_state>
</states>

```

Примеры соответствия типов:

ind:textfilecontent54_test → ind:textfilecontent54_object → ind:textfilecontent54_state

linux:dpkginfo_test → linux:dpkginfo_object

linux:rpminfo_test → linux:rpminfo_object

unix:file_test → unix:file_object → unix:file_state

unix:sysctl_test → unix:sysctl_object → unix:sysctl_state

windows:registry_test → windows:registry_object → windows:registry_state

windows:passwordpolicy_test → windows:passwordpolicy_object →
windows:passwordpolicy_state

windows:lockoutpolicy_test → windows:lockoutpolicy_object → windows:lockoutpolicy_state

windows:userright_test → windows:userright_object → windows:userright_state

windows:auditeventpolicysubcategories_test → windows:auditeventpolicysubcategories_object
→ windows:auditeventpolicysubcategories_state

windows:wmi57_test → windows:wmi57_object → windows:wmi57_state

Требования к variables

Если проверка использует переменные, они должны быть описаны в секции `variables`.

Допускается использование переменных, необходимых для работы поддерживаемых типов OVAL-тестов.

Переменная должна иметь уникальный идентификатор и использоваться только в рамках связанной OVAL-проверки.

Пример XCCDF- и OVAL- файла

Ниже приведен пример согласованной пары файлов:

- benchmark-xccdf.xml – бенчмарк с одним профилем соответствия и одним правилом;
- checks-oval.xml – OVAL-файл с одной проверкой соответствия, на которую ссылается правило из XCCDF-файла.

benchmark-xccdf.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<Benchmark xmlns="http://checklists.nist.gov/xccdf/1.1"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  id="xccdf_custom_benchmark_windows"
  xml:lang="ru-RU"
  resolved="0"
  style="SCAP_1.1">
  <status>accepted</status>
  <title>Пользовательский бенчмарк Windows</title>
  <description>Бенчмарк содержит пользовательский профиль проверки конфигурации ОС Windows.</description>
  <version>1.0</version>
  <Profile id="xccdf_custom_profile_windows">
    <title>Пользовательский профиль Windows</title>
    <description>Профиль включает проверку параметра парольной политики Windows.</description>
    <select idref="xccdf_custom_rule_password_history" selected="true"/>
  </Profile>
  <Rule id="xccdf_custom_rule_password_history" selected="false">
    <title>Принудительное использование истории паролей</title>
    <description>Необходимо убедиться, что система хранит историю ранее использованных паролей.</description>
    <ident system="custom_requirements">REQ.1</ident>
    <check system="http://oval.mitre.org/XMLSchema/oval-definitions-5">
      <check-content-ref href="checks-oval.xml" name="oval:custom:def:1"/>
    </check>
  </Rule>
</Benchmark>
```

checks-oval.xml

```
<?xml version="1.0" encoding="UTF-8"?>
<oval_definitions xmlns="http://oval.mitre.org/XMLSchema/oval-definitions-5"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:oval="http://oval.mitre.org/XMLSchema/oval-common-5"
  xmlns:windows="http://oval.mitre.org/XMLSchema/oval-definitions-5#windows">
  <generator>
    <oval:product_name>Custom</oval:product_name>
    <oval:schema_version>5.11.2</oval:schema_version>
    <oval:timestamp>2026-01-01T00:00:00Z</oval:timestamp>
    <oval:product_version>1.0</oval:product_version>
  </generator>
  <definitions>
    <definition id="oval:custom:def:1" version="1" class="compliance">
      <metadata>
        <title>Принудительное использование истории паролей</title>
        <description>Проверяется, что значение параметра password_hist_len больше или равно 24.</description>
        <affected family="windows">
          <platform>Windows 10</platform>
          <platform>Windows 11</platform>
          <platform>Windows Server 2019</platform>
          <platform>Windows Server 2022</platform>
        </affected>
      </metadata>
      <criteria>
        <criterion test_ref="oval:custom:tst:1"
          comment="Проверка значения password_hist_len"/>
      </criteria>
    </definition>
  </definitions>
  <tests>
    <windows:passwordpolicy_test id="oval:custom:tst:1"
      version="1"
      check="all"
      check_existence="at_least_one_exists"
      comment="Проверка значения парольной политики password_hist_len">
      <windows:object object_ref="oval:custom:obj:1"/>
      <windows:state state_ref="oval:custom:ste:1"/>
    </windows:passwordpolicy_test>
  </tests>
</oval_definitions>
```

```

    </windows:passwordpolicy_test>
</tests>
<objects>
  <windows:passwordpolicy_object id="oval:custom:obj:1"
                                version="1"
                                comment="Информация о парольной политике"/>
</objects>
<states>
  <windows:passwordpolicy_state id="oval:custom:ste:1"
                                version="1"
                                comment="Ожидаемое значение password_hist_len">
    <windows:password_hist_len datatype="int"
                                operation="greater than or equal"
                                var_ref="oval:custom:var:1"/>
  </windows:passwordpolicy_state>
</states>
<variables>
  <constant_variable id="oval:custom:var:1"
                     version="1"
                     datatype="int"
                     comment="Минимальное значение истории паролей">
    <value>24</value>
  </constant_variable>
</variables>
</oval_definitions>

```

Журналирование событий

Kaspersky Vulnerability Management использует следующие способы записи событий:

- Журнал системного аудита. Содержит информацию о действиях пользователя с компонентами и задачами Kaspersky Vulnerability Management.
- Журналы работы компонентов решения. Содержат информацию о событиях, возникших во время работы компонентов Kaspersky Vulnerability Management.

Журнал событий системного аудита

По умолчанию журнал системного аудита расположен по пути `/var/log/kaspersky/vulnerability-management/<название компонента>/*.log`.

Записи журнала системного аудита могут содержать следующие поля:

- `ts`. Дата и время (UTC), когда совершено действие.
- `msg`. **Описание совершенного действия с префиксом [Audit]**.
 - Экспорт активов в CSV ([Audit] Export assets to CSV).
 - Указание значимости активов ([Audit] Set assets importance).
 - Импорт профилей соответствия ([Audit] Import compliance profile).
 - Удаление профилей соответствия ([Audit] Delete compliance profiles).
 - Запуск задачи Kaspersky Vulnerability Management через API ([Audit] Run task).

- Добавление шаблонов Nuclei через API ([Audit] Add templates).
- Удаление шаблонов Nuclei через API ([Audit] Delete templates).
- Добавление результатов безагентного сканирования активов в режиме черного ящика ([Audit] Add scan results).
- Экспорт уязвимостей в CSV-файл ([Audit] Export vulnerabilities to CSV).
- Создание шаблона отчета ([Audit] Create report template).
- Изменение шаблона отчета ([Audit] Update report template).
- Удаление шаблонов отчетов ([Audit] Delete report templates).
- Удаление отчетов ([Audit] Delete reports).
- `component` и `version`. Идентификатор и версия компонента, с которым связаны действия пользователя.
- `userID`. Идентификатор пользователя, совершившего действие.
- `actionType`. **Числовой идентификатор совершенного действия.**
 - 1. Экспорт активов в CSV ([Audit] Export assets to CSV).
 - 2. Указание значимости активов ([Audit] Set assets importance).
 - 3. Импорт профилей соответствия ([Audit] Import compliance profile).
 - 4. Удаление профилей соответствия ([Audit] Delete compliance profiles).
 - 5. Запуск задачи Kaspersky Vulnerability Management через API ([Audit] Run task).
 - 6. Добавление шаблонов Nuclei через API ([Audit] Add templates).
 - 7. Удаление шаблонов Nuclei через API ([Audit] Delete templates).
 - 8. Добавление результатов безагентного сканирования активов в режиме черного ящика ([Audit] Add scan results).
 - 9. Экспорт уязвимостей в CSV-файл ([Audit] Export vulnerabilities to CSV).
 - 11. Создание шаблона отчета ([Audit] Create report template).
 - 12. Изменение шаблона отчета ([Audit] Update report template).
 - 13. Удаление шаблонов отчетов ([Audit] Delete report templates).
 - 14. Удаление отчетов ([Audit] Delete reports).
- **Поля, специфичные для совершенного действия.**
 - `userID`. Идентификатор пользователя.
 - `assetIDs`. Разделенные через запятую внутренние идентификаторы активов.

- **importance**. Значимость актива: 0 – не определена, 1 – низкая, 2 – средняя, 3 – высокая, 4 – критичная.
- **strategy**. Способ задания значимости активов: **include** – значимость задается для активов с идентификаторами **assetIDs**; **exclude** – значимость задается для всех активов за исключением **assetIDs**.
- **benchmarkID**. Значение атрибута **id** элемента **Benchmark** в файле с расширением **XCCDF**.
- **benchmarkDbID**. Уникальный внутренний идентификатор загружаемого бенчмарка.
- **profileIDs**. Разделенные запятой уникальные идентификаторы удаленных профилей соответствия.
- **executionID**. Идентификатор сессии выполнения задачи. Хранится в базе данных **Kaspersky Vulnerability Management**, с его помощью можно найти больше информации про задачу.
- **templateIDs**. Разделенные запятой идентификаторы шаблонов **Nuclei**.
- **assetID**. Идентификатор актива.
- **taskID**. Идентификатор задачи для актива.
- **parentTaskID**. Идентификатор задачи сканирования.

Пример записи в журнале системного аудита:

```
{ "level": "info", "ts": "2025-11-21T16:47:53.862+0300", "msg": "[Audit] Set assets importance", "component": "vm_api", "version": "0.9.0.0", "userID": "123", "actionType": 2, "importance": 2, "strategy": "include", "assetID": "bd2a7e69-a6d6-4194-86ab-98f79f9b283f", "benchmarkID": "96d9b5a7-874c-4af0-bcfd-389e66954abf" }
```

По умолчанию **Kaspersky Vulnerability Management** хранит записи в журнале системного аудита в течение 30 дней.

Журналы событий компонентов решения

События работы компонентов Сетевой сканер, Private API и Worker записываются в файл, по умолчанию расположенный в директории `/var/log/kaspersky/vulnerability-management/<имя компонента>`, где в качестве имени компонента может быть `scanner`, `privateapi`, `worker`.

Значения по умолчанию параметров записи событий для каждого компонента решения закодированы, и не указаны в конфигурационных файлах:

- **log.level** – уровень детализации событий. Возможные значения: `debug`, `info`, `warning` и `error`. По умолчанию установлено значение `info`.
- **log.filename** – полный путь к журналу событий компонента.
- **log.writer.file.maxsizeMb** – максимальный размер файла журнала событий в мегабайтах перед ротацией. По умолчанию равен 1000 МБ.
- **log.writer.file.maxbackups** – максимальное количество резервных копий журнала работы компонента, полученных в результате ротации. По умолчанию равно трем.

- `log.writer.file.maxagedays` – срок хранения журнала работы компонента. По умолчанию равно 30.
- `log.writer.file.uncompressed` – определяет, нужно ли оставлять без сжатия ротируемые файлы журналов работы компонентов. По умолчанию установлено значение `false` – файлы подвергаются сжатию.
- `log.writer.file.localtime` – определяет, нужно ли использовать системное время в формате UTC для форматирования отметки времени в резервных файлах журналов работы компонентов. По умолчанию используется.

Вы можете добавить перечисленные выше параметры с другими значениями в конфигурационные файлы компонентов `scanner.json`, `privateapi.json` и `worker.json`, расположенные в директории `/etc/kaspersky/vulnerability-management/configs/`. Пути к параметрам необходимо преобразовать в формат JSON. Например, значения параметров `log.writer.file.maxsizeb` и `log.writer.file.maxbackups` в конфигурационном файле должно быть записано следующим образом:

```
"log": {
  "writer.file": {
    "maxsizeb": 1000,
    "maxbackups": 3
  }
}
```

Проверка целостности модулей Kaspersky Vulnerability Management

Kaspersky Vulnerability Management содержит множество бинарных модулей в виде исполняемых файлов. Злоумышленники могут заменить один или несколько исполняемых файлов решения другими файлами, содержащими вредоносный код. Чтобы избежать подмены исполняемых файлов, предусмотрена проверка целостности Kaspersky Vulnerability Management с помощью утилиты `integrity_checker`. При запуске модулей Kaspersky Vulnerability Management утилита проверяет исполняемые файлы на наличие неавторизованных изменений или повреждений. Если исполняемый файл решения имеет некорректную контрольную сумму, то он считается поврежденным.

Утилита `integrity_checker` проверяет целостность исполняемых файлов Kaspersky Vulnerability Management на основе файла манифеста `vm_integrity_manifest.xml`, расположенного в директории `/opt/kaspersky/vulnerability-management/utls`. Утилита проверяет также целостность файла манифеста.

Настоятельно не рекомендуем вносить изменения в файл манифеста `vm_integrity_manifest.xml`, так как это сделает цифровую подпись недействительной и проверка целостности завершится ошибкой.

Чтобы запустить проверку целостности модулей Kaspersky Vulnerability Management вручную:

1. Откройте терминал.
2. На устройстве с установленными компонентами Kaspersky Vulnerability Management перейдите в директорию `/opt/kaspersky/vulnerability-management`:

```
cd /opt/kaspersky/vulnerability-management
```

3. Выполните команду:

```
sudo /opt/kaspersky/vulnerability-management/utils/integrity_checker ./utils/vm_integrity_manifest.xml  
[параметры]
```

Параметры утилиты `integrity_checker`:

- `--help` – вывести на экран справку утилиты.
- `--version` – вывести на экран версию утилиты.
- `--verbose` – вывести на экран дополнительную информацию о работе утилиты.

Результаты проверки целостности модулей Kaspersky Vulnerability Management выводятся в терминале в следующем виде:

- `SUCCEEDED` – целостность подтверждена.
- `FAILED` – целостность не подтверждена.

Удаление решения

Удаление Kaspersky Vulnerability Management состоит из следующих этапов:

- 1 [Выключение решения в Агентах администрирования активов](#)
- 2 [Выключение решения на Сервере администрирования Kaspersky Security Center](#)
- 3 [Удаление компонентов Kaspersky Vulnerability Management](#)
- 4 Удаление ролей и учетных записей пользователей, [созданных для решения](#)
- 5 [Удаление веб-плагина для управления решением через Kaspersky Security Center Web Console](#)

Выключение Kaspersky Vulnerability Management в Агентах администрирования активов

Агент администрирования Kaspersky Security Center участвует в [инвентаризации активов](#) и [анализе соответствия активов внутренним, отраслевым и регуляторным требованиям безопасности](#). Необходимая функциональность включена в Агентах администрирования активов в процессе развертывания решения.

Чтобы выключить функциональность Kaspersky Vulnerability Management в Агентах администрирования:

1. В главном окне Web Console выберите **Управление активами** → **Политики**.
2. Откройте политику с настройками для Агента администрирования Kaspersky Security Center, в которой включена функциональность Kaspersky Vulnerability Management.
3. Откройте вкладку **Параметры приложения**.

4. В разделе **Обновления и уязвимости в приложениях** переведите переключатель **Включить Kaspersky Vulnerability Management** в неактивное положение.

5. Нажмите на кнопку **Сохранить**.

После применения измененной политики функциональность Kaspersky Vulnerability Management будет выключена в Агентах администрирования, установленных на устройствах, входящих в группу Kaspersky Security Center **Управляемые устройства**.

Выключение Kaspersky Vulnerability Management на Сервере администрирования

Чтобы выключить функциональность Kaspersky Vulnerability Management на Сервере администрирования Kaspersky Security Center:

1. На устройстве с установленным Сервером администрирования выполните следующую команду:

```
/opt/kaspersky/ksc64/sbin/klscflag -fset -pv ".core/.independent" -s klcsff -n KLCS_FF_VMGMT_SUPPORT -t d -v 0
```

2. На устройстве с установленным Сервером администрирования Kaspersky Security Center перезапустите службу Сервера администрирования с помощью следующей команды:

```
systemctl restart kladminserver_srv.service
```

Удаление компонентов Kaspersky Vulnerability Management

[Компоненты Kaspersky Vulnerability Management](#) обеспечивают основные функции решения.

Чтобы удалить компоненты Kaspersky Vulnerability Management:

1. На устройстве с установленным Kaspersky Vulnerability Management откройте терминал.

2. Выполните одну из команд:

- `sudo apt remove --purge kaspersky-vm` – в операционных системах, использующих формат пакетов `.deb`;
- `sudo dnf remove kaspersky-vm` – в операционных системах, использующих формат пакетов `.rpm`;
- `sudo apt-get remove --purge kaspersky-vm` – в операционных системах семейства Альт.

Удаление веб-плагина для управления решением

Чтобы удалить веб-плагин для управления решением через Kaspersky Security Center Web Console:

1. В главном окне Web Console выберите **Параметры** → **Веб-плагины**.

Откроется список установленных веб-плагинов.

2. В списке веб-плагинов установите флажок около Kaspersky Vulnerability Management.

3. Нажмите на кнопку **Удалить**.

4. В открывшемся окне с предложением сохранить резервную копию плагина перед удалением нажмите на кнопку **ОК** или **Пропустить резервное копирование данных**.

Веб-плагин Kaspersky Vulnerability Management будет удален. Раздел **Управление уязвимостями** главного меню Web Console будет скрыт.

Работа с публичным API решения

Для получения данных от Kaspersky Vulnerability Management другие решения могут использовать публичный API Kaspersky Vulnerability Management – VM REST API. Среди решений АО "Лаборатория Касперского" Kaspersky SIEM использует VM REST API для получения от Kaspersky Vulnerability Management данных об активах и найденных уязвимостях.

VM REST API — это HTTP-интерфейс, который позволяет клиентскому приложению с помощью запросов и ответов запрашивать и получать данные от Kaspersky Vulnerability Management. Запросы и ответы передаются по HTTP-протоколу в формате JSON.

Запросы к VM REST API формируются с помощью методов. Вы можете ознакомиться с методами VM REST API [по ссылке](#).

Каждый запрос к VM REST API должен включать авторизацию с использованием токена сессии и сопровождаться заголовком `X-KSC-Session: <токен_сессии>`. Для создания токена сессии необходимо вызвать метод [Session.StartSession](#) KSC Open API.

Запросы к VM REST API необходимо отправлять по адресу `https://<VM API FQDN>:<номер порта>/<версия VM REST API>/<имя метода>`, где VM API FQDN – полное доменное имя сервера, на котором установлены компоненты Kaspersky Vulnerability Management. Например: `https://example.com:5054/v1/assets`.

Пример запроса с помощью утилиты curl:

```
curl -k --location --request POST 'https://example.com:5054/v1/assets' \
--header 'Content-Type: application/json' \
--header 'X-KSC-Session: <токен_сессии>' \
--data ''
```

Обращение в Службу технической поддержки

Если вы не нашли решения вашей проблемы в документации или других [источниках информации о Kaspersky Vulnerability Management](#), рекомендуется обратиться в Службу технической поддержки. Сотрудники Службы технической поддержки ответят на ваши вопросы об установке и использовании Kaspersky Vulnerability Management.

"Лаборатория Касперского" предоставляет поддержку Kaspersky Vulnerability Management в течение жизненного цикла (см. [страницу жизненного цикла приложений](#) [↗]). Прежде чем обратиться в Службу технической поддержки, ознакомьтесь с [правилами предоставления технической поддержки](#) [↗].

Вы можете связаться со специалистами Службы технической поддержки одним из следующих способов:

- [посетить сайт Службы технической поддержки](#) [↗];
- отправить запрос в Службу технической поддержки "Лаборатории Касперского" с [портала Kaspersky CompanyAccount](#) [↗].

Источники информации о решении

Указанные источники информации о решении (в частности, онлайн-справка) созданы для удобства пользователя и не являются полноценным эквивалентом этого документа.

Страница Kaspersky Vulnerability Management на веб-сайте "Лаборатории Касперского"

На [странице Kaspersky Vulnerability Management](#) [↗] вы можете получить общую информацию о решении, его возможностях и особенностях работы.

База знаний и онлайн-справка

База знаний – это раздел на веб-сайте Службы технической поддержки "Лаборатории Касперского".

На [странице Kaspersky Vulnerability Management в Базе знаний](#) [↗] вы найдете статьи, которые содержат полезную информацию, рекомендации и ответы на часто задаваемые вопросы о приобретении, установке и использовании решения.

Статьи в Базе знаний могут дать ответы на вопросы, связанные с Kaspersky Vulnerability Management и с другими приложениями "Лаборатории Касперского". Также в статьях Базы знаний могут быть новости Службы технической поддержки.

Для отображения онлайн-справки требуется соединение с интернетом.

Если вы не нашли решения вашего вопроса, обратитесь в [Службу технической поддержки](#).

Юридическая информация

В этом разделе приведена юридическая информация.

Лицензирование решения

Kaspersky Vulnerability Management распространяется с ограниченным сроком использования. Информация о предоставлении пользователю права на использование решения содержится в Лицензионном соглашении.

О Лицензионном соглашении

Лицензионное соглашение – это юридическое соглашение между вами и АО "Лаборатория Касперского", в котором указано, на каких условиях вы можете использовать приложение.

Внимательно ознакомьтесь с условиями Лицензионного соглашения перед началом работы с приложением.

Вы можете ознакомиться с условиями Лицензионного соглашения следующими способами:

- Прочитав текст файла license.<идентификатор языка>. Этот файл включен в [комплект поставки решения](#).
- Во время [установки компонентов Kaspersky Vulnerability Management](#).

Вы принимаете условия Лицензионного соглашения, подтверждая свое согласие с текстом Лицензионного соглашения во время установки компонентов Kaspersky Vulnerability Management. Если вы не согласны с условиями Лицензионного соглашения, установка компонентов Kaspersky Vulnerability Management прерывается.

- После установки решения Kaspersky Vulnerability Management.

После установки решения файл с текстом Лицензионного соглашения решения расположен на устройстве в директории `/opt/kaspersky/vulnerability-management/doc/license.<идентификатор языка>`.

О лицензии

Лицензия – это ограниченное по времени право на использование решения, предоставляемое вам на основании Лицензионного соглашения.

Объем предоставляемых услуг и срок использования решения зависят от типа лицензии, по которой используется решение.

О Лицензионном сертификате

Лицензионный сертификат – это документ, в котором содержится следующая информация о предоставляемой лицензии:

- идентификатор лицензии или номер заказа;
- информация о пользователе, которому предоставляется лицензия;
- информация о решении, которое можно активировать по предоставляемой лицензии;
- ограничение на количество единиц лицензирования (например, количество обрабатываемых событий в секунду);
- дата начала срока действия лицензии;
- дата окончания срока действия лицензии или срок действия лицензии;
- тип лицензии.

Предоставление данных

Данные, передаваемые в АО "Лаборатория Касперского"

Данные для обновления баз уязвимостей. Полученная информация защищается "Лабораторией Касперского" в соответствии с установленными законом требованиями и действующими правилами "Лаборатории Касперского". Данные передаются по зашифрованным каналам связи.

Данные, обрабатываемые локально

Для выполнения своих основных функций Kaspersky Vulnerability Management может принимать, хранить и обрабатывать следующие данные:

- Характеристики активов. Kaspersky Vulnerability Management получает данные об активах от Сервера администрирования Kaspersky Security Center. Пользователь видит описание активов в интерфейсе Kaspersky Security Center Web Console:
 - Параметры актива, необходимые для идентификации: идентификатор в базе данных, имя и описание, IPv4-адрес или IPv6-адрес, DNS-имя и DNS-домен, ID и версия Агента администрирования, NetBIOS-имя.
 - Прочие характеристики актива: тип, последнее появление в сети, дата добавления актива в систему, операционная система и ее архитектура, номер сборки операционной системы, значимость актива, Windows-домен, тип виртуальной машины, производитель материнской платы, версия прошивки материнской платы.

- Данные об открытых портах и службах на активе. Kaspersky Vulnerability Management получает данные с помощью Сетевого сканера, установленного в сети. Пользователь может ознакомиться с результатами сканирования в интерфейсе Kaspersky Security Center Web Console: список открытых портов, протоколы, для которых открыты порты; службы, доступные через открытые порты; дата и время последнего сканирования активов.
- Данные результатов анализа активов на соответствие стандартам. Анализ выполняет модуль анализа соответствия. Результаты анализа передаются Агентом администрирования в Kaspersky Vulnerability Management. Пользователь может ознакомиться с результатами анализа соответствия в интерфейсе Kaspersky Security Center Web Console: идентификаторы правил и профилей соответствия, названия и описания правил и профилей соответствия, названия стандартов, способ добавления профилей соответствия в базу, ссылки на нормативные документы профилей соответствия, дата и время добавления профилей соответствия в Kaspersky Vulnerability Management, список покрываемых мер, дата и время последнего сканирования активов.
- Данные об обнаруженных на активах уязвимостях. Kaspersky Vulnerability Management получает данные об уязвимостях с помощью модуля обнаружения уязвимостей и Сетевого сканера. Пользователь может ознакомиться с обнаруженными уязвимостями в интерфейсе Kaspersky Security Center Web Console: названия и описания уязвимостей, внутренние и внешние идентификаторы уязвимостей, оценка и уровень опасности уязвимостей, приоритет устранения уязвимостей, источники уязвимостей и рекомендации по их устранению, наличие эксплойта, PoC и сетевого вектора атаки в уязвимостях; трендовость уязвимостей, CWE, EPSS, дата публикации, показатель возможности эксплуатации уязвимости нарушителями, метод обнаружения уязвимости, дата первого и последнего обнаружения, затронутое уязвимостями программное обеспечение и активы, на которых оно установлено.
- Данные об установленном программном обеспечении на активах. Kaspersky Vulnerability Management получает данные о программном обеспечении с помощью модуля обнаружения программного обеспечения. Данные передаются Агентом администрирования в Kaspersky Vulnerability Management. Решение также получает инвентарные данные о ПО путем сканирования активов в режиме белого ящика. Пользователь может ознакомиться с данными об обнаруженном программном обеспечении в интерфейсе Kaspersky Security Center Web Console: название и описание, версия, поставщик, тип, дата и время первого появления, размер, путь установки, обнаруженные уязвимости, активы, на которых установлено ПО.
- Файлы логов компонентов Kaspersky Vulnerability Management. Файлы логов не передаются в АО "Лаборатория Касперского" автоматически, но администратор может передать эти файлы в "Лабораторию Касперского" вручную по запросу для решения проблем в работе Kaspersky Vulnerability Management.
- Данные, необходимые для установки Kaspersky Vulnerability Management и интеграции с Сервером администрирования Kaspersky Security Center.
- Данные, необходимые для авторизации запросов к публичному API.
- Данные, необходимые для запуска сканирования активов в режиме белого ящика.
- Информация о принятии пользователем условий юридического соглашения с "Лабораторией Касперского".
- Учетные данные для аутентификации пользователей Kaspersky Vulnerability Management.
- Любые данные, которые пользователь вводит в интерфейсе веб-плагина для управления решением Kaspersky Vulnerability Management через Kaspersky Security Center Web Console.

Перечисленные выше данные хранятся в СУБД, к которой пользователь подключает Kaspersky Vulnerability Management, или в конфигурационных файлах. Срок хранения данных в СУБД определяется пользователем.

Более подробная информация об обработке, хранении и уничтожении информации, полученной во время использования решения и переданной в "Лабораторию Касперского", приведена в Политике конфиденциальности на [веб-сайте "Лаборатории Касперского"](#) .

Информация о стороннем коде

Информация о стороннем коде содержится в файле `legal_notices.txt`, расположенном в директории `/opt/kaspersky/vulnerability-management/doc/`.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe, Acrobat, ColdFusion, Flash, Illustrator, Photoshop, Reader, Shockwave является либо зарегистрированным товарным знаком, либо товарным знаком компании Adobe в США и/или других странах.

Apache, Apache Cassandra, Apache Flink, Apache HTTP Server, Apache Solr, Apache Spark, Apache Struts, Apache Tomcat, OFBIZ являются либо зарегистрированными товарными знаками, либо товарными знаками Apache Software Foundation в Соединенных Штатах и/или других странах.

Atlassian, Atlassian Confluence – зарегистрированный товарный знак ATlassian PTY LTD.

Red Hat, Red Hat Enterprise Linux – товарные знаки или зарегистрированные в США и других странах товарные знаки Red Hat, Inc. или дочерних компаний.

Google, Chrome, Chromium, Google Chrome, Google Earth, Google Earth Pro, Vite – товарные знаки Google LLC.

Cisco, Cisco Jabber, Jabber являются зарегистрированными товарными знаками или товарными знаками Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

ClickHouse является зарегистрированным товарным знаком ClickHouse, Inc. <https://clickhouse.com/>

Debian – зарегистрированный товарный знак Software in the Public Interest, Inc.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Dropbox – товарный знак Dropbox, Inc.

EaseUS Todo Backup – зарегистрированный товарный знак Chengdu Yiwo Tech Development Co., Ltd.

Electrum – зарегистрированный товарный знак Electrum Technologies GmbH.

Evernote – зарегистрированный товарный знак Evernote Corporation.

GITLAB – товарный знак GitLab Inc. в США и других странах и регионах.

Mozilla, Firefox, Thunderbird являются товарными знаками Mozilla Foundation в США и других странах.

FORTICLIENT – товарный знак правообладателя Fortinet, Inc.

Foxit – зарегистрированный товарный знак Foxit Corporation.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

GITHUB – – товарный знак GitHub, Inc., зарегистрированный в США и других странах.

IrfanView – зарегистрированный товарный знак Skiljan, Irfan.

iTunes – товарный знак Apple Inc.

JetBrains – товарный знак JetBrains s.r.o.

JOOMLA! – товарный знак Open Source Matters, Inc.

Linux – товарный знак Linus Torvalds, зарегистрированный в США и в других странах.

MariaDB – зарегистрированный товарный знак MariaDB Corporation.

MongoDB – зарегистрированный товарный знак MONGODB, INC.

minio – зарегистрированный товарный знак Minio, Inc.

Nginx – зарегистрированный товарный знак NGINX, Inc.

Node.js – товарный знак Joyent, Inc.

Microsoft, Excel, Internet Explorer, Microsoft Edge, Microsoft Teams, OneNote, Outlook, PowerPoint, Project, SharePoint, Visual Studio, Windows Server, Word являются товарными знаками группы компаний Microsoft.

OpenSSL является товарным знаком правообладателя OpenSSL Software Foundation.

OpenVPN – зарегистрированный товарный знак OpenVPN, Inc.

openSUSE – зарегистрированный товарный знак SUSE LLC.

Oracle, Oracle Virtualbox – зарегистрированный товарный знак компании Oracle и/или аффилированных компаний.

PostgreSQL – зарегистрированный товарный знак The PostgreSQL Global Development Group.

Python – товарный знак или зарегистрированный товарный знак Python Software Foundation.

Radmin – зарегистрированный товарный знак Famatech.

Redis – товарный знак Redis Ltd.

Rocky Linux является товарным знаком The Rocky Enterprise Software Foundation.

TeamViewer – зарегистрированный товарный знак Teamviewer GmbH.

Telegram – зарегистрированный товарный знак Telegram Messenger LLP.

Ubuntu является зарегистрированным товарным знаком Canonical Ltd.

WooCommerce – товарный знак Automattic Inc.

Zabbix – зарегистрированный товарный знак Zabbix SIA.

2GIS – зарегистрированный товарный знак ООО "ДубльГИС".

Альт – зарегистрированный товарный знак ООО "Альт-Инвест".

РЕД ОС – зарегистрированный товарный знак ООО "Ред Софт".

Глоссарий

kvm-group

Группа с правами на чтение конфигурационных файлов решения. Создается во время установки компонентов Kaspersky Vulnerability Management. Пользователи, входящие в эту группу, получают доступ на чтение конфигурационных файлов решения в соответствии с правами группы.

OVAL

OVAL (Open Vulnerability and Assessment Language) – открытый язык описания и оценки уязвимостей.

XCCDF

XCCDF (The Extensible Configuration Checklist Description Format) – основанный на XML формат описания контрольных списков параметров безопасности.

Вероятность EPSS

Вероятность эксплуатации уязвимости в реальных условиях в ближайшие 30 дней.

Группа администрирования

Набор устройств, объединенных в Kaspersky Security Center в соответствии с выполняемыми функциями и устанавливаемым на них набором приложений "Лаборатории Касперского". Устройства группируются для удобства управления ими как единым целым. В состав группы администрирования могут входить другие группы. Для каждого из установленных в группе администрирования приложений могут быть созданы групповые политики и сформированы групповые задачи.

Групповая задача

Задача, назначенная для группы администрирования и выполняемая на всех управляемых устройствах, входящих в состав группы.

Приоритет устранения уязвимости

Приоритет устранения уязвимости по методике ФСТЭК – это оценка, показывающая, насколько срочно конкретную уязвимость необходимо устранить именно в вашей ИТ-инфраструктуре.

Методика ФСТЭК дополняет техническую оценку CVSS контекстом ИТ-инфраструктуры организации. Согласно действующей методике ФСТЭК, при определении приоритета устранения уязвимости учитываются следующие параметры:

- оценка уязвимости по CVSS;
- тип и количество затронутых активов;
- влияние затронутых активов на защищенность ИТ-инфраструктуры организации;
- сведения об эксплуатации уязвимости и наличии эксплойта;
- возможные последствия эксплуатации.

Возможные значения приоритета устранения уязвимости:

- Критичный;
- Высокий;
- Средний;
- Низкий.

Чем выше приоритет устранения уязвимости, тем быстрее рекомендуется устранить ее.

Профиль соответствия

Набор написанных в соответствии со спецификациями OVAL и XCCDF правил, в которых описаны условия для соответствия активов внутренним, отраслевым и регуляторным требованиям безопасности. Правила профиля соответствия объединены общей темой и помещены в один XML-файл.

Процентиль EPSS

Процент уязвимостей, имеющих такую же или более низкую вероятность эксплуатации.

Сервер администрирования

Компонент приложения Kaspersky Security Center, осуществляющий функции централизованного хранения информации об установленных в сети организации приложениях "Лаборатории Касперского" и управления ими.

Уровень опасности уязвимости

Показатель того, насколько серьезную угрозу представляет уязвимость. Определяется по числовой оценке CVSS. Если доступны оценки по нескольким версиям CVSS, используется оценка самой новой версии.

Возможные значения уровня опасности уязвимости:

- *Низкий* — соответствует числовой оценке CVSS от 0,0 до 3,9 включительно;
- *Средний* — соответствует числовой оценке CVSS от 4,0 до 6,9 включительно;
- *Высокий* — соответствует числовой оценке CVSS от 7,0 до 9,9 включительно;
- *Критический* — соответствует числовой оценке CVSS, равной 10,0.

Чем выше уровень опасности уязвимости, тем быстрее рекомендуется устранить ее.

Уязвимость

Недостаток в операционной системе или приложении, который может быть использован злоумышленниками для проникновения в операционную систему или приложение и нарушения их целостности. Большое количество уязвимостей в операционной системе делает ее работу ненадежной, так как внедрившиеся в операционную систему вредоносные программы могут вызывать сбои в работе как самой операционной системы, так и установленных приложений.