

Задачи KES для Windows 12.8 - Standard

Задача поиск вредоносного ПО KES Windows 12.8 (Быстрая) - Standard

- **Тип задачи:** Поиск вредоносного ПО
- **Расписание:**
 - Ежедневно (быстрая проверка) - 12:00
- Запускать пропущенные задачи - **включить**
- Использовать автоматическое определение случайного интервала между запусками задачи - **включить**
- **Уведомление**
 - На сервере администрирования - **15 суток**
 - Хранить в журнале событий ОС на устройстве - **включить**
 - Сохранять все события - **включить**
 - Сохранять информацию о результатах
- **Настройки**
 - Типы файлов - **Файлы, проверяемые по формату**
 - Оптимизация - Проверять только новые и измененные файлы - **включить**
 - Оптимизация - Пропускать файлы, если их проверка длится более **180 сек**
 - Проверка составных файлов
 - Проверять архивы - **включить**
 - Проверять дистрибутивы - **включить**
 - Проверять файлы, офисных форматов - **включить**
 - Проверять файлы почтовых форматов - **выключить**
 - Проверять архивы, защищенные паролем - **выключить**
 - Дополнительно - Не распаковывать составные файлы, большого размера - **включить**
 - Максимальный размер файла - **100 МБ**

- Методы проверки:
 - Эвристический анализ - **включить** (поверхностный)
 - Технологии проверки:
 - Технология iSwift - **включить**
 - Технология iChecker - **включить**
 - Документы - **включить**
 - Моя почта - **выключить**
 - Память ядра - **включить**
 - Запущенные процессы и объекты автозапуска - **включить**
 - Загрузочные секторы - **включить**
 - Системное резервное хранилище - **выключить**
 - Все съемные диски - **включить**
 - Все жесткие диски - **включить**
 - Все сетевые диски - **выключить**
 - Уровень безопасности - **Другой**
 - Область проверки:
 - Режим запуска - Выполнять только во время простоя компьютера - **выключить**
 - Не запускать несколько задач проверки одновременно - **включить**
 - Действия при обнаружении угрозы - **Лечить. Удалять, если лечение не возможно**
 - Выполнять лечение активного заражения немедленно - **включить**
-

Задача поиск вредоносного ПО KES Windows 12.8 (Полная) - Standard

- **Тип задачи:** Поиск вредоносного ПО
- **Расписание:**
 - Еженедельно (Полная проверка) - **Понедельник, 15:00**
- Запускать пропущенные задачи - **включить**
- Использовать автоматическое определение случайного интервала между запусками задачи - **включить**
- **Уведомление**
 - На сервере администрирования - **15 суток**
 - Хранить в журнале событий ОС на устройстве - **включить**
 - Сохранять все события - **включить**

- Сохранять информацию о результатах

• Настройки

- Типы файлов - **Все файлы**
 - Оптимизация - Проверять только новые и измененные файлы - **ВЫКЛЮЧИТЬ**
 - Уровень безопасности - **Высокий**

 - Оптимизация - Пропускать файлы, если их проверка длится более - **ВЫКЛЮЧИТЬ**
 - Проверка составных файлов
 - Проверять архивы - **включить**
 - Проверять дистрибутивы - **включить**
 - Проверять файлы, офисных форматов - **включить**
 - Проверять файлы почтовых форматов - **включить**
 - Проверять архивы, защищенные паролем - **выключить**
 - Дополнительно - Не распаковывать составные файлы, большого размера - **выключить**

 - Методы проверки:
 - Эвристический анализ - **включить** (глубокий)

 - Технологии проверки:
 - Технология iSwift - **включить**
 - Технология iChecker - **включить**

 - Область проверки:
 - Документы - **включить**
 - Моя почта - **включить**
 - Память ядра - **включить**
 - Запущенные процессы и объекты автозапуска - **включить**
 - Загрузочные секторы - **включить**
 - Системное резервное хранилище - **выключить**
 - Все съемные диски - **включить**
 - Все жесткие диски - **включить**
 - Все сетевые диски - **выключить**

 - Режим запуска - Выполнять только во время простоя компьютера - **выключить**
 - Не запускать несколько задач проверки одновременно - **включить**
 - Действия при обнаружении угрозы - **Лечить. Удалять, если лечение не возможно**
 - Выполнять лечение активного заражения немедленно - **включить**
-

Задача обновления антивирусных баз и модулей KES Windows 12.8 - Standard

- **Тип задачи:** «Обновление»
 - **Периодичность:** Каждые 60 минут
 - **Источник обновлений:**
 - Сервера Kaspersky в интернете
 - **Уведомление**
 - Сохранять информацию о результатах
 - На сервере администрирования - **15 суток**
 - Хранить в журнале событий ОС на устройстве - **включить**
 - Сохранять все события - **включить**
 - **Настройки**
 - Источник обновлений - **Серверы обновлений "Лаборатории Касперского"**
 - Загружать обновления модулей приложений - **включить**
 - Устанавливать критические и одобренные обновления - **включить**
 - Настройки обновлений в мобильном режиме - **Серверы обновлений "Лаборатории Касперского"**
 - Загружать обновления модулей приложений - **включить**
 - Устанавливать только одобренные обновления - **включить**
-

Задача инвентаризации KES Windows 12.8 - Standard

- **Тип задачи:** Инвентаризация
- **Уведомление**
 - Сохранять информацию о результатах
 - На сервере администрирования - **15 суток**
 - Хранить в журнале событий ОС на устройстве - **включить**

- Сохранять все события - **включить**
 - **Расписание:**
 - Еженедельно - **Пятница. 15:00**
 - **Области инвентаризации:** **%SystemRoot%, %ProgramFiles%, %ProgramFiles(x86)%**
 - Выполнять только во время простоя компьютера - **выключить**
 - Инвентаризация DLL-модулей - **выключить**
 - Инвентаризация файлов скриптов - **выключить**
 - Дополнительно - Проверять только новые и измененные файлы - **включить**
 - Дополнительно - Проверять архивы - **выключить**
 - Дополнительно - Проверять дистрибутивы - **включить**
 - Дополнительно - Не распаковывать составные файлы большого размера - **включить**
 - Максимальный размер файла **100 МБ**
-

Задача запуска KES Windows 12.8 - Standard

- **Тип задачи:** Запуск Kaspersky Endpoint Security
 - **Расписание:**
 - Ежедневно - 11:55
 - Запускать пропущенные задачи - **включить**
 - Использовать автоматическое определение случайного интервала между запусками задачи - **включить**
 - **Параметры**
 - Kaspersky Endpoint Security для Windows (12.8.0) - **включить**
 - Запустить приложение - **включить**
-

Задача поиска уязвимостей и требуемых обновлений KES Windows

12.8 - Standard

- **Тип задачи:** «Поиск уязвимостей и обновлений»
- **Расписание**
 - По дням недели: **Вторник, Четверг**
 - Время запуска **14:00**
 - Запускать пропущенные задачи - **включить**
 - Использовать автоматическое определение случайного интервала между запусками задач - **включить**
- **Параметры**
 - Поиск уязвимостей и обновлений, перечисленных Microsoft - **включить**
 - Соединяться с сервером обновлений для актуализации данных - **включить**
 - Поиск уязвимостей и сторонних обновлений, перечисленных "Лабораторией Касперского" - **включить**
 - Пути для дополнительного поиска приложений в файловой системе:
 - **%SystemRoot%**
 - **%ProgramFiles%**
 - **%ProgramFiles(x86)%**
 - Включить расширенную диагностику - **выключить**

Расширенная диагностика. Если этот параметр включен, Агент администрирования будет записывать трассировку, даже если трассировка выключена для Агента администрирования в утилите удаленной диагностики Kaspersky Security Center. Трассировка записывается в два файла по очереди; размер каждого файла равен половине значения указанного в поле Максимальный размер файлов расширенной диагностики, МБ. Когда оба файла заполняются, Агент администрирования начинает записывать данные поверх. Файлы трассировки хранятся в папке %WINDIR%\Temp

Задача установки требуемых обновлений и закрытия уязвимостей

KES Windows 12.8 - Standard

- **Общие**

-

- Распределить по подгруппам - **включить**

- **Уведомления**

-

- Сохранять информацию о результатах
 - На сервере администрирования в течении (сут) - **15**
- Сохранять все события - **включить**

- **Расписание**

- Каждую неделю - **Среда**
- Время запуска - **13:00**
- Использовать автоматическое определение случайного интервала между запусками задачи - **включить**

- **Параметры**

-

- Задача по закрытию уязвимостей:
 - **Устанавливать все обновления, кроме отклоненных**
 - Закрывать уязвимости с уровнем критичности, равным или выше - **Средний**
 - Общие критерии
 - Обновления - **Устанавливать все подходящие обновления**
 - Уязвимости - **Закрывать все уязвимости, соответствующие остальным критериям**
- Начинать установку в момент перезагрузки или выключения устройства - **выключить**
- Устанавливать требуемые общесистемные компоненты - **включить**
- Разрешать установку новой версии приложения при обновлении - **включить**
- Загружать обновления на устройство, не устанавливая их - **выключить**
- Включить расширенную диагностику - **выключить**

- **Первоначальная установка**

- - **Не проверять** (но как вариант можно использовать группу Low)

- **Перезагрузка операционной системы**

- - Действие после установки обновления, при необходимости перезагрузки - **Запрашивать у пользователя**
 - Повторять запрос каждые (мин) - **60**
 - Принудительно перезагрузить (мин) - **выключить**
 - Принудительное закрытие приложения в заблокированных сессиях через (мин) - **выключить**

Revision #1

Created 18 June 2025 18:59:09 by admin_mf

Updated 18 June 2025 18:59:46 by admin_mf