



Kaspersky Endpoint Security 8 для Windows
Kaspersky Security Center

KASPERSKY lab

Вместо вступления

Основные тенденции в области цифровых угроз

- Рост числа угроз
- При этом сложность зловредов неуклонно возрастает
- Уязвимости – главный путь осуществления атак
- Плюс социальная инженерия
- Атаки не только на Windows!
- Основная цель: кража информации или создание ботнетов
- В результате – получение прибыли

Основные тенденции в области цифровых угроз

- Вектор атак смещается в сторону корпоративных пользователей, государственных органов и промышленных объектов
- Основные цели: кража конфиденциальной информации, выведение из строя сегментов корпоративной сети, шантаж, шпионаж

Проникновение

Извне

- через браузер
- через другие Интернет-службы (email, instant messenger, и др.)
- **используя уязвимости ПО**
- **используя социальную инженерию**



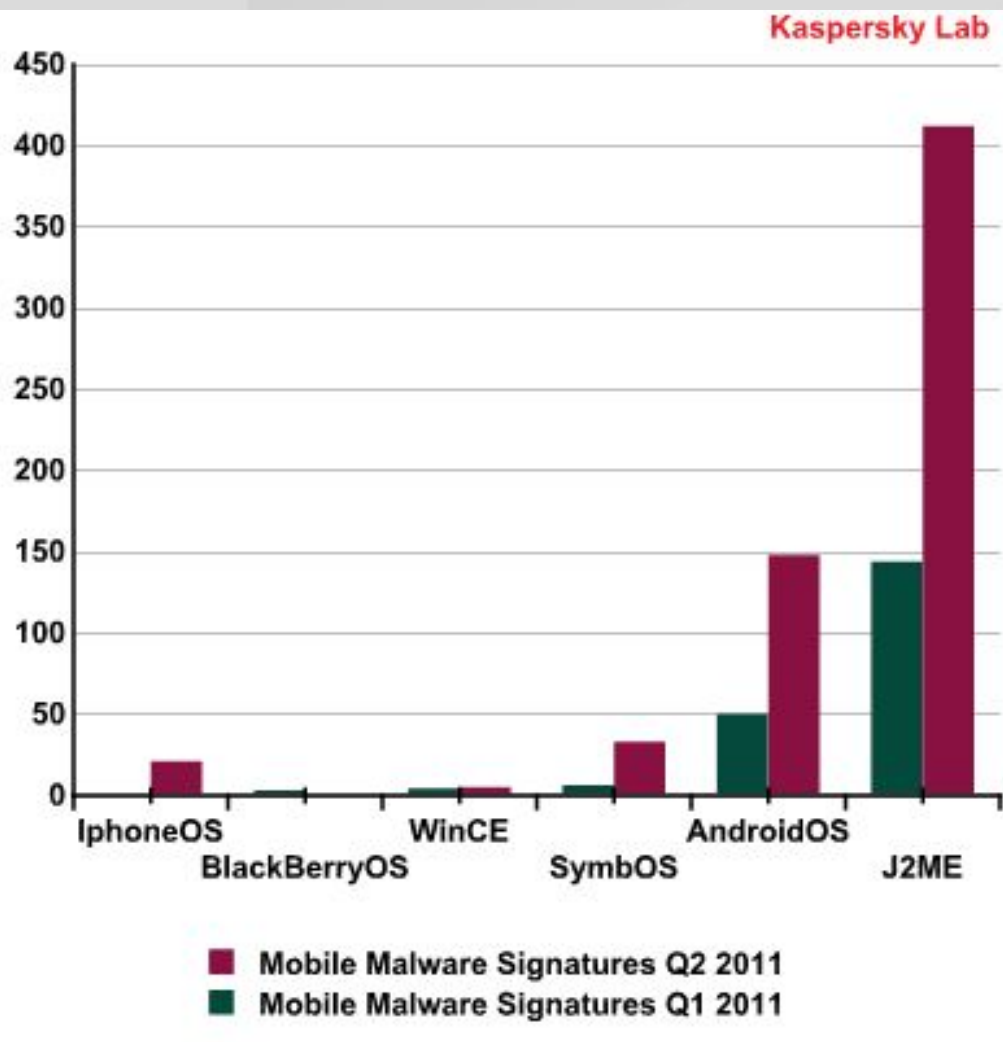
Изнутри

- через зараженные устройства (съемные диски, мобильные устройства)
- **используя соц. инженерию**
- **с помощью инсайдеров**

Уязвимости – бич современных информационных систем

- ✓ Новые уязвимости появляются ежедневно
- ✓ Патчи появляются с большой задержкой
- ✓ Да и не все их инсталлируют
- ✓ Уязвимости - они повсюду!

Мобильные устройства: у каждого с собой?



- Использование «классической» коммуникации с использованием центра; зловердами схемы командного центра;
- Сообщения системы безопасности, появляющиеся в момент запуска и установки любого приложения, в абсолютном большинстве случаев пользователем игнорируются;
- Существует возможность обхода систем контроля приложений

Deja vu?



KASPERSKY Lab

Выводы

- Нет оснований рассчитывать на то, что в ближайшем будущем ситуация с кибер-преступностью изменится к лучшему
- Очевидно, что Интернет-преступлений будет все больше и больше

Что делать?

Для сотрудников и системных администраторов

Базовые правила безопасности

- Информирование сотрудников об актуальных угрозах
- Принуждение использовать безопасные пароли
- Принуждение к регулярной смене паролей
- Использование защищенных протоколов
- Максимальное ограничение привилегий сотрудников

- Регулярное обновление серверных систем
- Регулярное обновление ПО на рабочих станциях
- Проведение тестов на проникновение в инфраструктуру
- Использование комплексных решений защиты



Kaspersky Endpoint Security 8 для Windows

Kaspersky Endpoint Security 8 для Windows

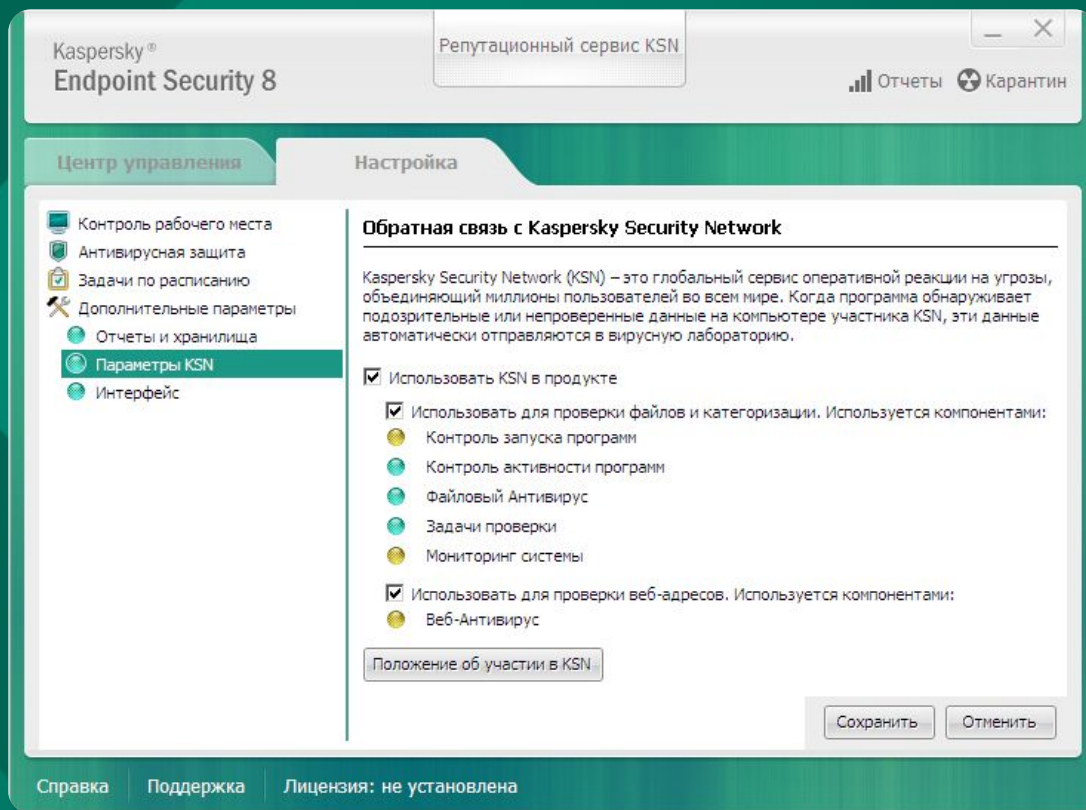
Защита от угроз сегодняшнего и завтрашнего дня

- ▶ Защита рабочих мест
 - Сигнатурный анализ
 - Проактивная защита
 - Облачная защита (Kaspersky Security Network)
- ▶ Контроль рабочих мест
 - Контроль программ
 - Контроль устройств
 - Веб-Контроль



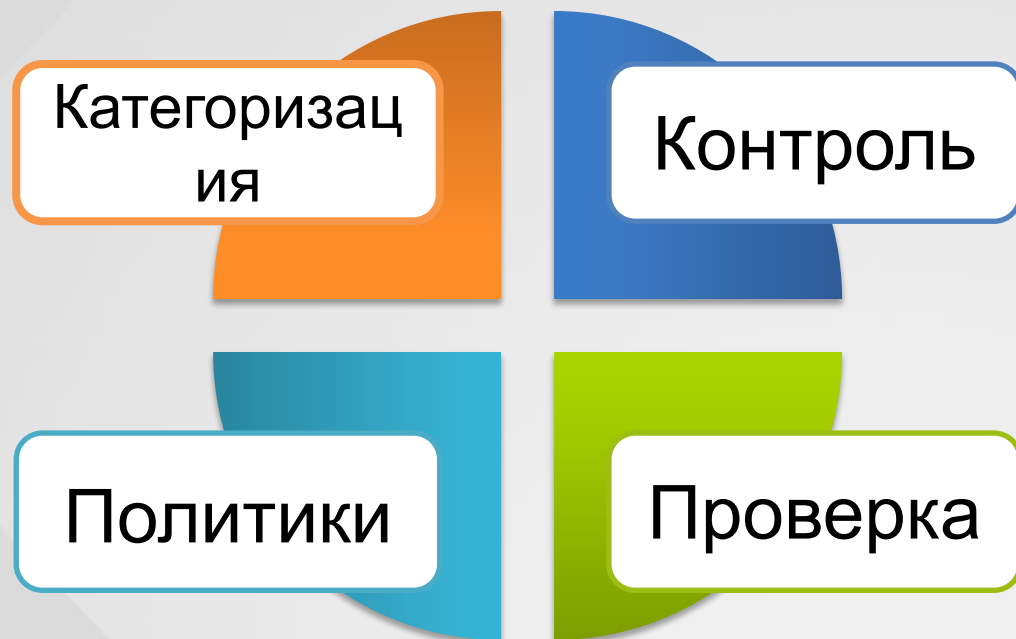
Kaspersky Security Network (KSN)

- ▶ Облачная репутационная база
- ▶ Информация о 3 миллиардах объектов
- ▶ Мгновенное детектирование угроз и быстрое реагирование
- ▶ Минимальный риск ложных срабатываний



Контроль программ

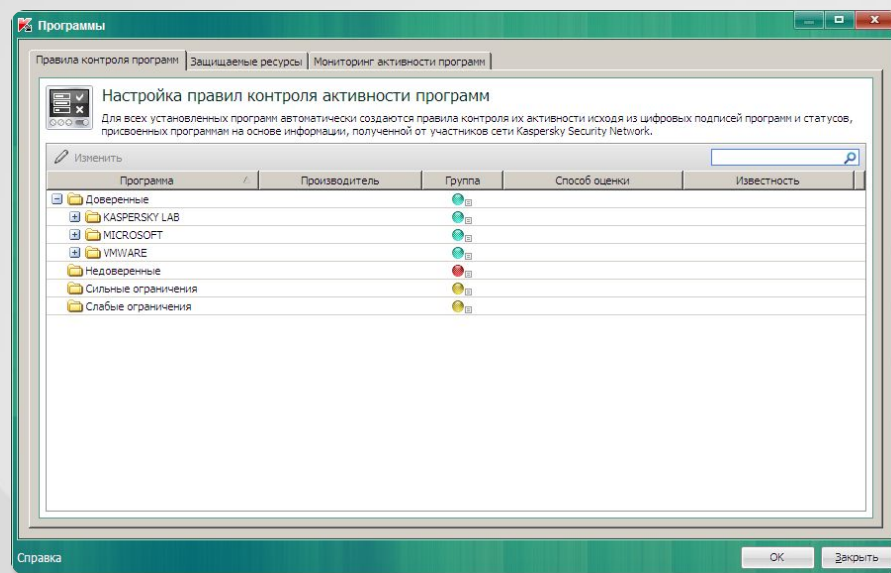
- ▶ Категоризация программ и белые списки
- ▶ Контроль запуска программ
- ▶ Контроль активности программ
- ▶ Мониторинг уязвимостей



Категоризация программ и белые списки

- ▶ Предустановленные KL-категории
 - созданные специалистами «Лаборатории Касперского»
- ▶ Собственные категории
 - созданные администратором
- ▶ Локальный и облачный белые списки
- ▶ Непрерывный мониторинг

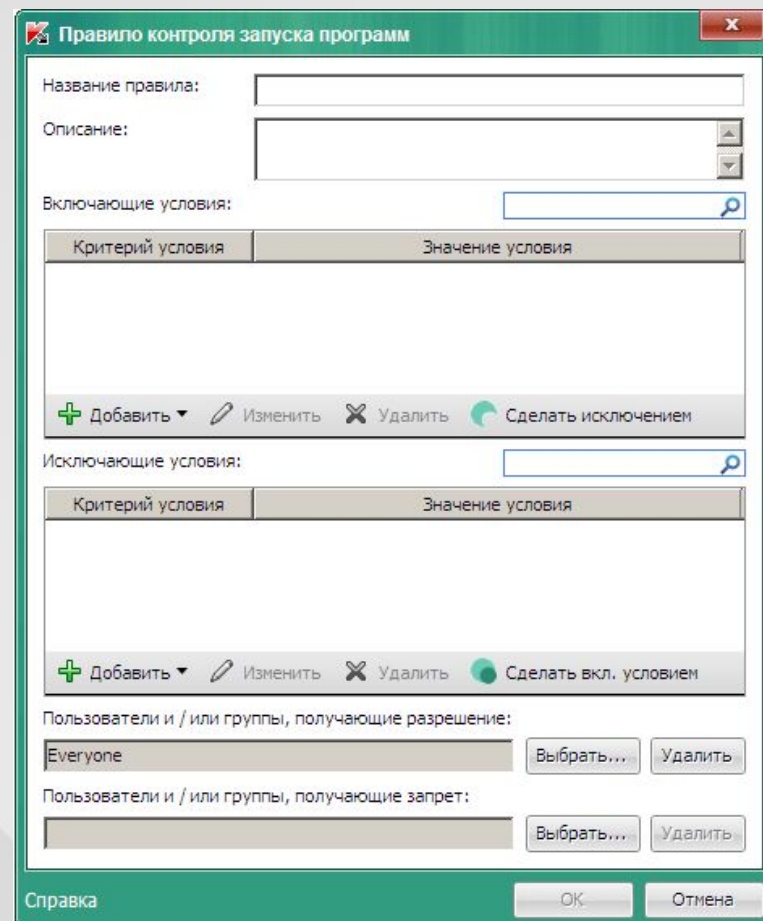
Категоризация



Контроль запуска программ

Контроль

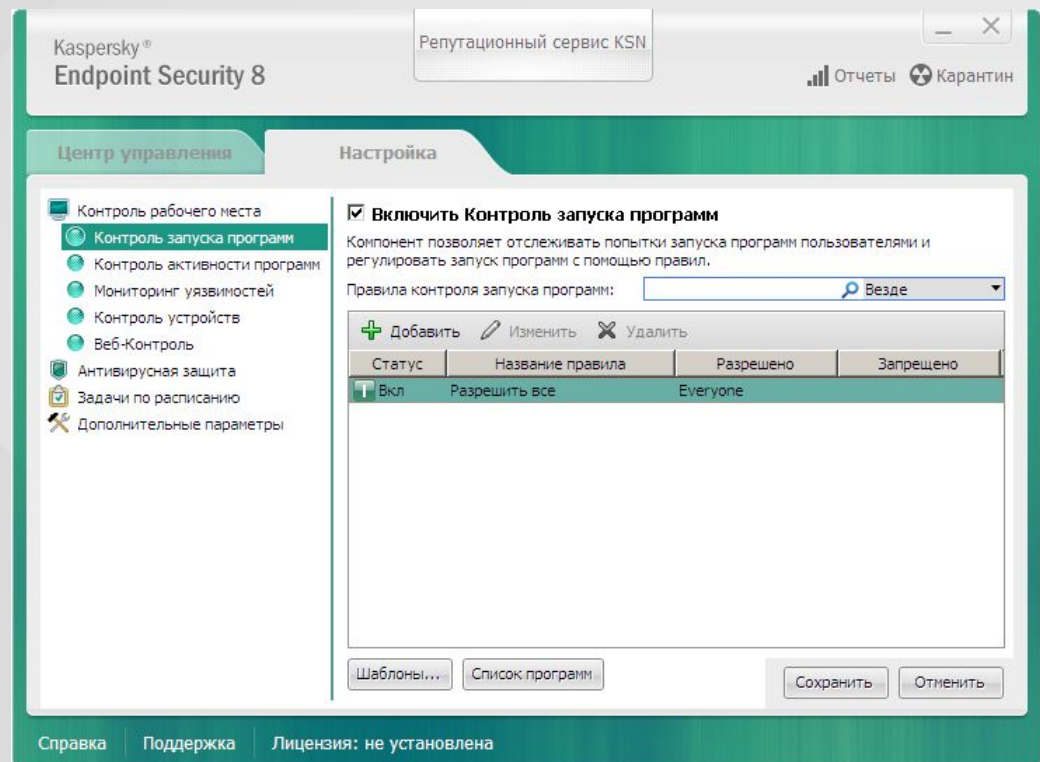
- ▶ Аудит запуска программ
- ▶ Разрешение и блокирование по белым спискам и категориям
- ▶ Интеграция с Active Directory
- ▶ Экономия сетевых ресурсов



Контроль активности программ

Политик
и

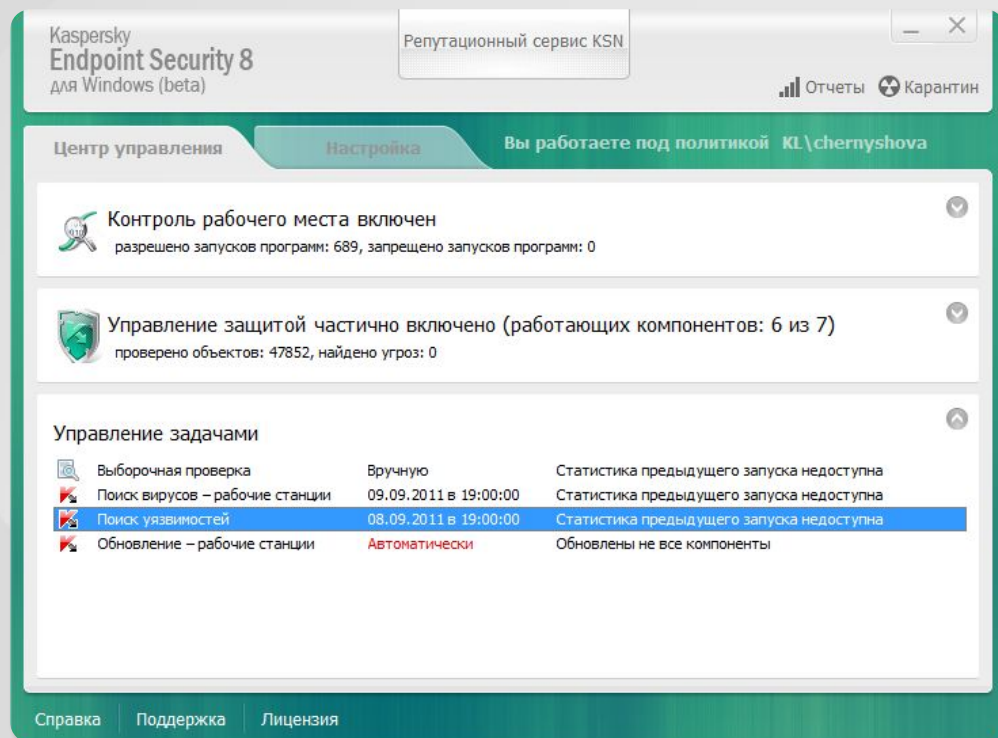
- ▶ Применение правил к запущенным программам
- ▶ Автоматическое распределение программ по группам:
 - Доверенные
 - Слабые ограничения
 - Сильные ограничения
 - Недоверенные
- ▶ Выбор политики в зависимости от присвоенной категории и группы
- ▶ Ограничение работы программ с:
 - реестром
 - ресурсами системы
 - данными пользователя
- ▶ Снижение вероятности использования в сети нежелательного ПО



Мониторинг уязвимостей

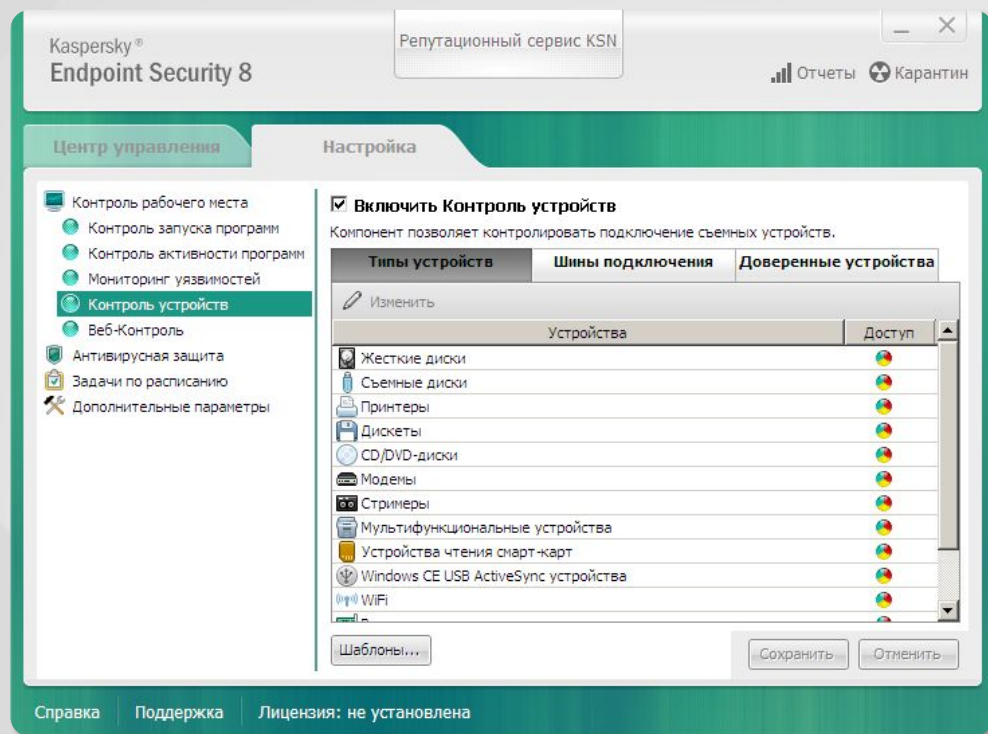
Проверка
а

- ▶ Проверка программ на наличие уязвимостей
- ▶ 3 источника данных:
 - база уязвимостей компании Secunia
 - список уязвимостей приложений Microsoft
 - список уязвимостей, составленный специалистами «Лаборатории Касперского»
- ▶ Задачи мониторинга:
 - информация
 - предупреждение
 - «первая помощь»
- ▶ Повышение надежности защиты



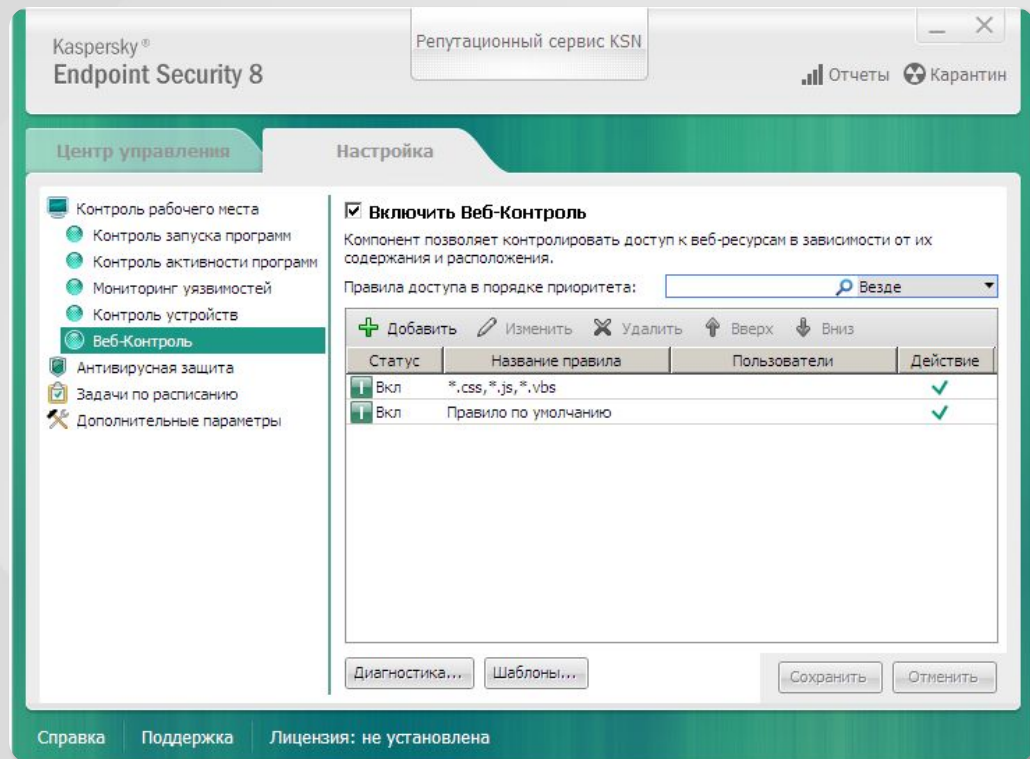
Гранулярный контроль устройств

- ▶ Ограничение доступа к подключаемым устройствам
 - внешние жесткие диски и другие накопители, модемы, принтеры
- ▶ Ограничение доступа по:
 - Типу устройства
 - Способу подключения (шине)
 - Серийному номеру
- ▶ Поддержка идентификаторов устройств
- ▶ Настройка расписания для применения правил



Веб-Контроль

- ▶ Аудит использования веб-ресурсов
- ▶ Политики доступа к веб-ресурсам:
 - Разрешение, запрещение или ограничение доступа
 - Расписание применения политик
 - Интеграция с Active Directory
- ▶ Правила доступа к веб-ресурсам по параметрам
- ▶ Тестирование правил
- ▶ Интеграция с KSN: использование репутационных сервисов для проверки ссылок



Другие улучшения

- ▶ Улучшенная защита и лечение заражений
 - Мониторинг системы
 - Технология обновляемых шаблонов опасного поведения (BSS, Behavior Stream Signatures)
 - Откат вредоносных действий
- ▶ Улучшенный сетевой экран
- ▶ Система обнаружения вторжений (IDS)
 - Поддержка исключений по IP-адресам
- ▶ Проверка трафика по протоколам:
 - IRC
 - Mail.Ru
 - AIM



Функциональные возможности в защите рабочих станций и файловых серверов

Функции	Kaspersky Endpoint Security 8 для Windows	
	Рабочие станции	Файловые серверы
Файловый Антивирус	+	+
Почтовый Антивирус	+	-
Веб-Антивирус	+	-
IM-Антивирус	+	-
Технология лечения активного заражения (Advanced disinfection)	+	-
Мониторинг системы	+	-
Проактивная защита	+	-
Мониторинг активности программ: технология UDS (KSN)	+	-
Мониторинг активности программ: репутационная база KSN	+	-
Сетевой экран	+	+
Система обнаружения вторжений (IDS)	+	+
Контроль программ	+	-
Контроль устройств	+	-
Веб-Контроль	+	-
Мониторинг уязвимостей	+	+
Интеграция с KSN	+	+

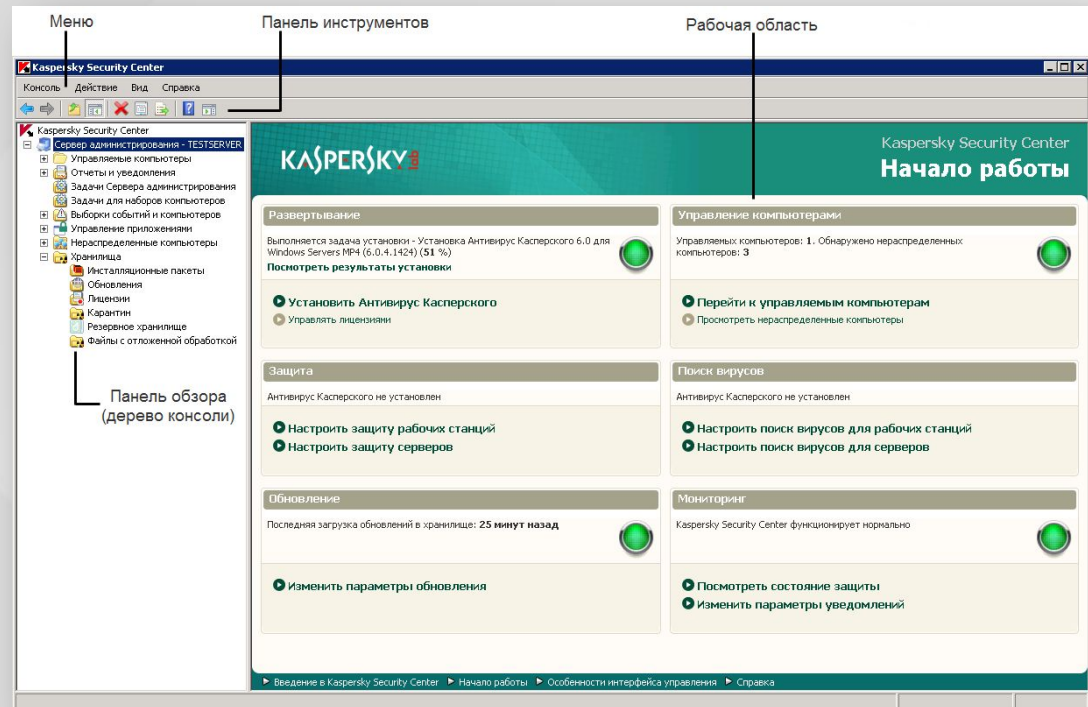


Kaspersky Security Center

Kaspersky Security Center

НОВЫЕ ВОЗМОЖНОСТИ

- ▶ Управление виртуальными машинами VMware
- ▶ Создание виртуальных Сервером администрирования
- ▶ Инвентаризация программных и аппаратных средств
- ▶ Поиск уязвимостей
- ▶ Служба KSN Proxy
- ▶ Веб-консоль



Kaspersky Endpoint Security 8 для Windows и Kaspersky Security Center

- ▶ Ключевые и преимущества

Ключевые преимущества: Kaspersky Endpoint Security 8 для Windows



- ▶ Усиленная защита благодаря сочетанию проактивных, сигнатурных и облачных технологий
- ▶ Минимальный риск ложных срабатываний
- ▶ Мощные инструменты для контроля рабочего места:
 - контроль устройств
 - веб-контроль
 - контроль запуска программ
 - контроль активности программ / белые списки
- ▶ Полная интеграция с Kaspersky Security Center 9

Ключевые преимущества: Kaspersky Security Center



- ▶ Централизованное управление комплексной системой защиты
- ▶ Оперативное развертывание системы защиты
- ▶ Поддержка иерархической структуры управления
- ▶ Специальные политики для мобильных пользователей
- ▶ Просмотр состояния защиты при помощи веб-консоли
- ▶ Информационные панели и система отчетов
- ▶ Поддержка мультиплатформенных сред
- ▶ Автоматическая поддержка жизненного цикла виртуальных машин

Спасибо!

<http://www.kaspersky.ru>

<http://www.securelist.com/ru>

KASPERSKY lab