Технологии и продукты Microsoft в обеспечении ИБ

Лекция 15. Защита от вирусных угроз

Цели

- Рассмотреть типы информационных вирусов.
- Изучить основные типы антивирусных средств защиты – средства контроля целостности, антивирусные мониторы и сканеры, антивирусные шлюзы.
- Познакомиться с новыми подходами к построению антивирусных средств защиты
- Выявить основное отличие продукта Microsoft ForeFront от других антивирусных решений

Типы вирусных угроз

- [ГОСТ Р 51188-98] *Компьютерный вирус* - специально созданный программный код, способный самостоятельно распространяться в компьютерной среде
  - файловые и загрузочные вирусы
  - «сетевые черви»
  - бестелесные вирусы
  - комбинированный тип
- «Троянский конь» (Trojan Horses)
- Spyware
- Adware

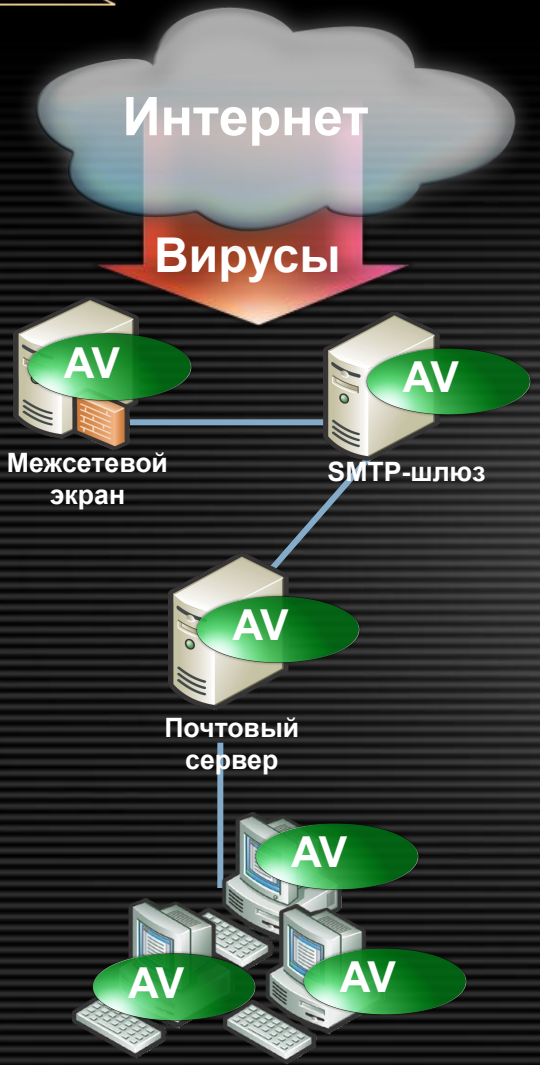
Модель нарушителя

№	Класс нарушителя	Степень преднамеренности действий нарушителя	Уровень квалификации нарушителя
1	Класс «Н-1»	Непреднамеренные действия	-
2	Класс «Н-2»	Преднамеренные действия	Низкий
3	Класс «Н-3»	Преднамеренные действия	Средний
4	Класс «Н-4»	Преднамеренные действия	Высокий

Модель защиты от потенциального нарушителя антивирусной безопасности

№	Класс нарушителя	Механизмы безопасности
1	Класс «Н-1»	Антивирусные продуты одного производителя
2	Класс «Н-2»	
3	Класс «Н-3»	Антивирусные продукты различных производителей
4	Класс «Н-4»	Антивирусные продукты различных производителей, средства межсетевого экранирования, средства обнаружения и предотвращения атак, обнаружения уязвимостей

Решение одного производителя



Одно и то же ядро сканирования используется на уровне шлюзов, серверов и рабочих станциях

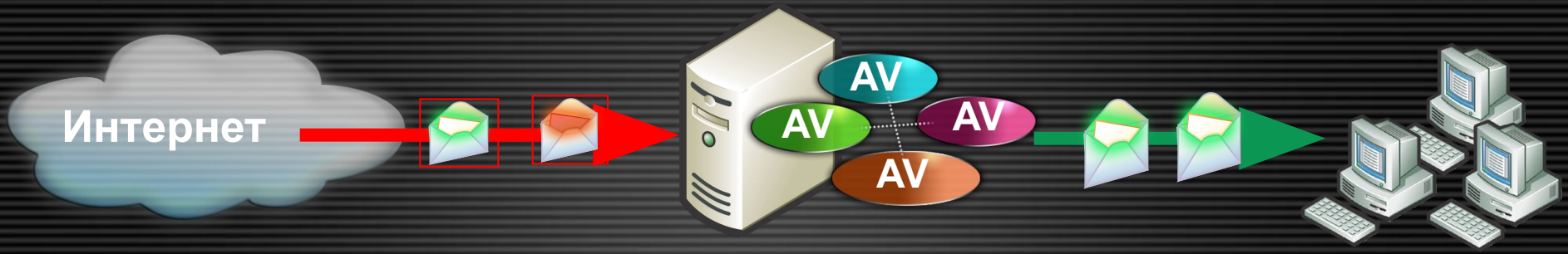
- **Недостатки подхода:**
  - Зависимость от одной антивирусной лаборатории
  - Неизбежность очередей и задержек на серверах по время обновления баз данных сигнатур антивирусного ПО
  - Одна точка уязвимости всей системы

Решения разных производителей

Для выявления вирусов используются различные продукты от разных производителей

Многоядерная антивирусная защита

MS Forefront



Exchange Server / Windows SMTP Server
Client Security / ISA / Intelligent Application Gateway
Share Point / Office Communications Server (H2.2007)

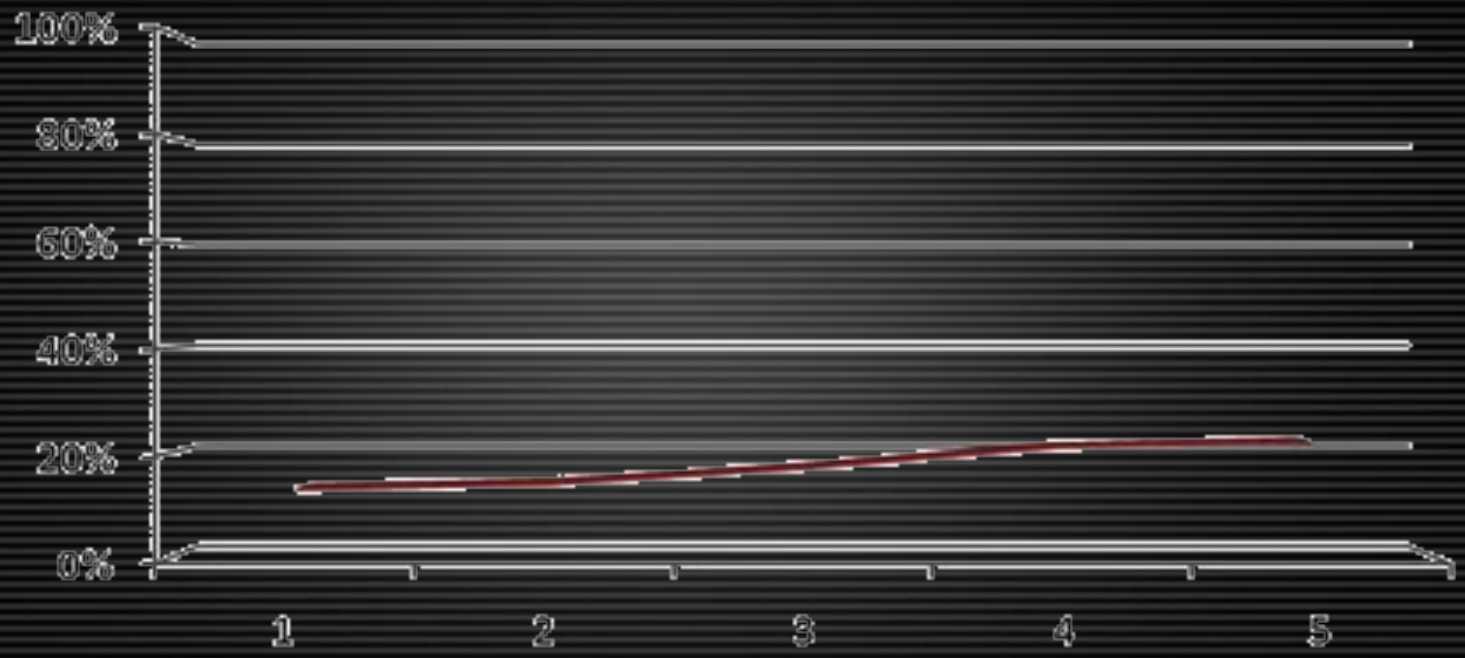
- централизованное управление несколькими серверами
- централизованное управление политиками

Ядра, входящие в состав Forefront

- До 9-ти антивирусных ядер одновременно из следующего списка:
  - Microsoft Antimalware engine
  - Sophos Virus Detection (Англия)
  - Computer Associates – Vet (Австралия)
  - Norman Data Defense (Швеция)
  - Computer Associates – Inoculate (Израиль)
  - Лаборатория Касперского (Россия)
  - Virus Buster (Венгрия)
  - Authentium Command Antivirus (США)
  - AhnLab (Южная Корея)

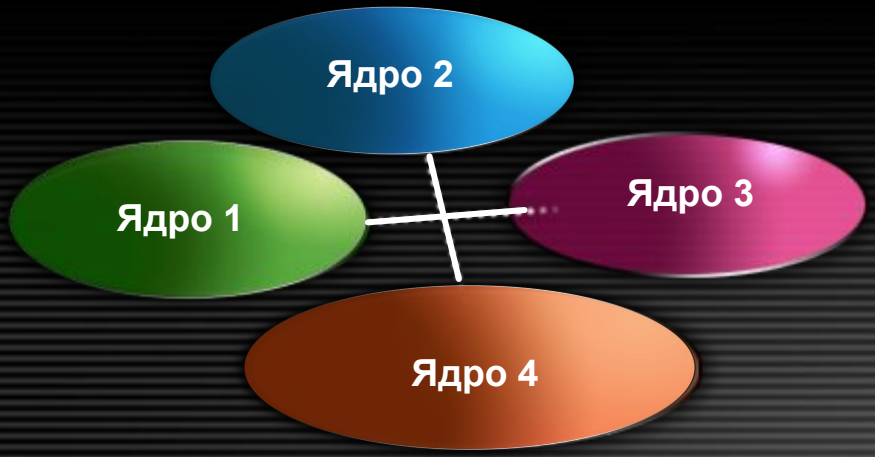
Загрузка процессора

Зависимость загрузки процессора
от количества антивирусных ядер



По результатам тестов компании **3Sharp** (октябрь, 2006)

Управление составом антивирусных ядер Forefront

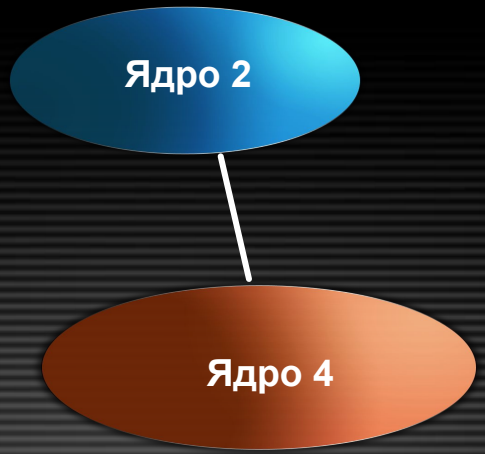


- **Максимум надёжности: использование всех имеющихся ядер (100%)**
- **Больше надёжности**: использование 75% ядер

- **Нейтральный выбор**: использование 50% ядер
- **Больше производительности**: использование 25% ядер
- **Максимум производительности**: использование одного ядра для каждого сканирования

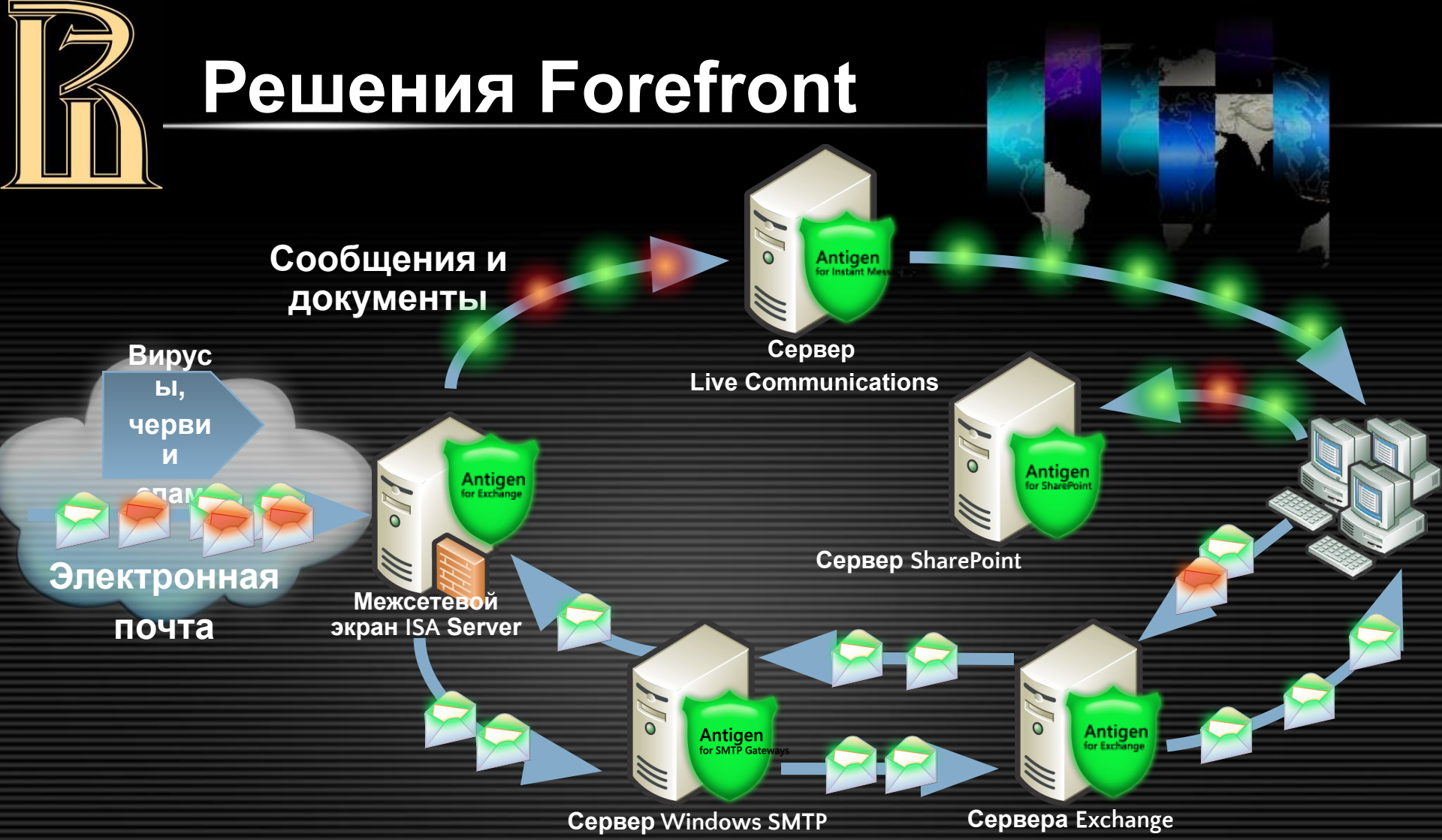
Управление составом антивирусных ядер Forefront

- **Максимум надёжности:** использование всех имеющихся ядер (100%)
- **Больше надёжности**: использование 75% ядер



- **Нейтральный выбор: использование 50% ядер**
- **Больше производительности**: использование 25% ядер
- **Максимум производительности**: использование одного ядра для каждого сканирования

Решения Forefront



Многоуровневая защита

Интеграция с инфраструктурой

Контроль контента

Microsoft Forefront

Microsoft® Forefront™

- Всесторонняя защита бизнес-приложений, позволяющая достичь лучшей защиты и безопасного доступа посредством глубокой интеграции и упрощенного управления

Защита клиентской и серверной ОС

Microsoft® Forefront™ Client Security

Защита серверных приложений

Microsoft® Forefront™ Security for Exchange Server

Microsoft® Forefront™ Security for SharePoint®

Microsoft® Forefront™ Server Security Management Console

Защита периметра

Microsoft® Internet Security & Acceleration Server 2006

Intelligent Application Gateway 2007

Forefront Client Security

- Обеспечение безопасности конечных точек (EndPoint Protection) = защита от вредоносного ПО + оценка здоровья
- Интеграция с существующей инфраструктурой (SQL, AD, GPO, WSUS)
- Высоко масштабируемое решение
- Продвинутая отчетность
- Низкая стоимость владения

Контроль и отчетность

“Соответствует ли моя инфраструктура рекомендациям по безопасности?”

“Как изменяется во времени уровень уязвимости системы?”

“Какая часть моей инфраструктуры наиболее уязвима?”

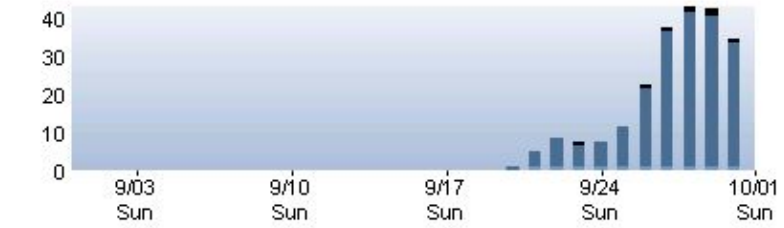
Security State Assessment Summary

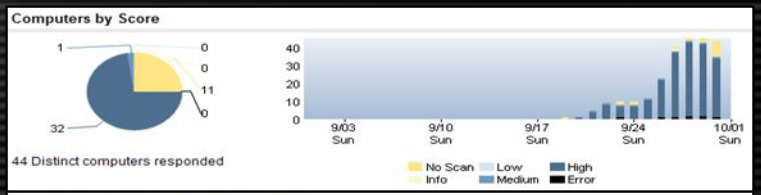
Top Vulnerabilities

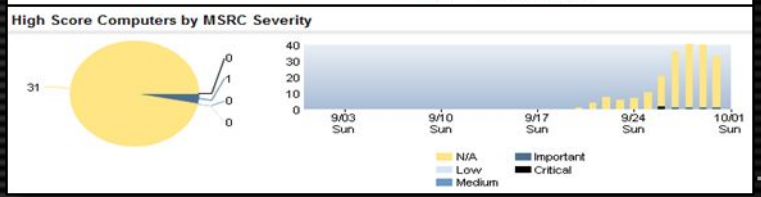
Name	Error	High	Medium
Passwords Expiration	0	31	0
MS06-000	0	9	0
File System	0	8	0
Autologon	0	3	0
Guest Account	0	1	0

Security State Assessment History

Vulnerabilities Discovered During the Last 30 Days

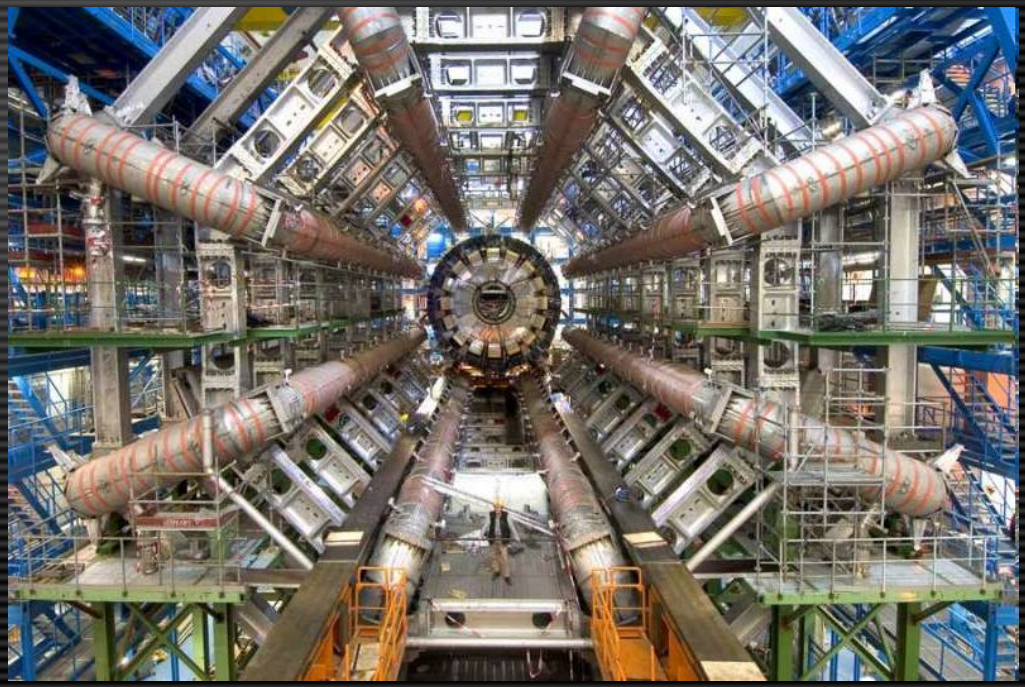






Forefront будет защищать большой адронный коллайдер

- ***CERN:*** *"By the end of this year, all NICE PCs will have MS Forefront Client Security installed. This new anti-virus and anti-malware application will replace the current anti-virus product from Symantec. The reasons for this change include the small footprint of the client application, excellent response times for pattern updates and very good integration with the existing NICE infrastructure."*



Microsoft Security Essentials

- Новый бесплатный пакет антивирусных приложений от компании Microsoft
- 23 июня 2009 года выпущена ограниченная публичная бета-версия продукта, доступная для скачивания только первым 75000 пользователям из США, Израиля и Бразилии
- Релиз финальной версии состоится осенью 2009 г.
- Будет представлен на 20 рынках и 10 языках.

Особенности Microsoft Security Essentials

- На ранней стадии разработки программа была известна под кодовым именем Morro
- Придет на смену коммерческому сервису Windows Live OneCare
- Microsoft Security Essentials включает в себя только движок по удалению вредоносных кодов
- Во время инсталяции MSE Windows Defender будет отключен
- Антивирусные базы для MSE будут выходить раз в сутки

4 уровня угрозы

- серьезная угроза
- высокий уровень
- средний уровень
- низкий уровень угрозы

Варианты сканирования

- Быстрый
  - сканирует лишь папку Windows и запущенные процессы
- Полный
- Выборочный
  - можно указать в каких папках произвести сканирование

Возможности

- Возможность удаления наиболее распространенных вредоносных программ
- Возможность удаления известных вирусов
- Антивирусная защита в реальном времени
- Возможность удаления известных шпионских программ
- Защита от шпионских программ в реальном времени.

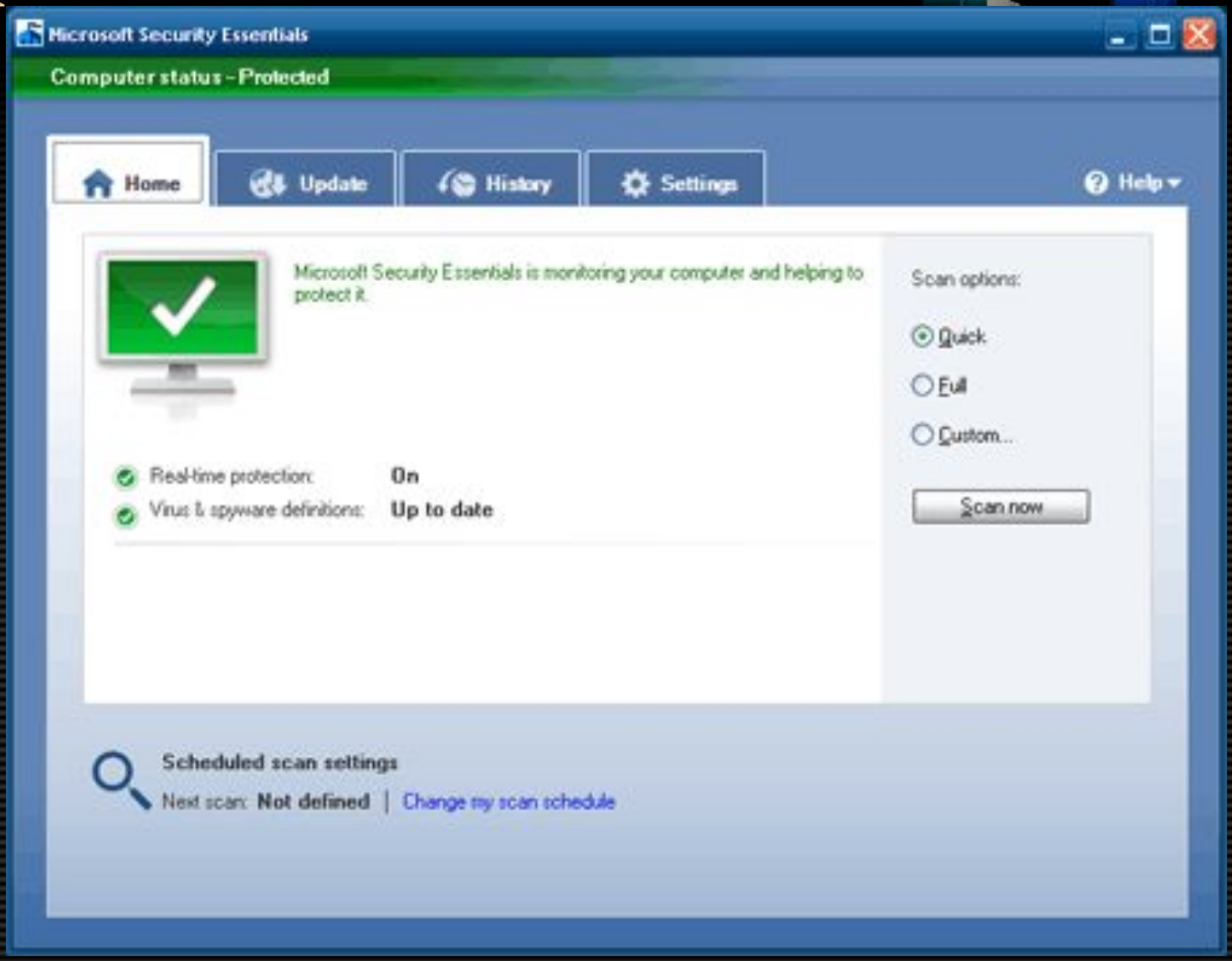
Производительность

- Ограничение загрузки процессора (в результате чего система всегда будет оставаться отзывчивой на запросы пользователя);
- Сканирование во время отдыха (сканирование и обновление будут иметь низкий приоритет и будут выполнять только во время отдыха компьютера);
- Умное кэширование и использование памяти (не используемые сигнатуры вирусов не загружаются в память).

Интерфейс

- Схож с Windows Defender
- 4 вкладки
  - **Home** - демонстрируются сведения о работе программы и актуальности антивирусных баз, а также представлены опции для выполнения быстрой, полной или частичной проверки компьютера на предмет наличия вредоносного программного обеспечения
  - **Update** - фигурирует одноимённая клавиша и отображаются сведения об обновлении приложения и антивирусных сигнатур
  - **History** - говорит само за себя, и в ней можно просмотреть историю работы пакета с указанием всех файлов, в которых найдены вирусы
  - **Settings** - представлены различные настройки антивируса.

Интерфейс


Microsoft Security Essentials
Computer status - Protected
Home
Update
History
Settings
Help
Microsoft Security Essentials is monitoring your computer and helping to protect it.
Real-time protection: On
Virus & spyware definitions: Up to date
Scan options:
Quick
Full
Custom...
Scan now
Scheduled scan settings
Next scan: Not defined | Change my scan schedule

Обнаружение вирусов

Тестирование MSE

- Компания AV-Test GmbH
  - Платформы: Windows XP, Vista и Windows 7
  - 3200 наиболее актуальных вирусов, троянов и червей
- Результат
  - "Все файлы были должным образом продиагностированы и вылечены. Это отличный результат, так как многие антивирусы до сих пор не определяют эти вирусы".
  - "Ни один из безопасных файлов не был помечен как вредоносный - это отличный результат".

Использованные источники

- **Сердюк В.А.** Комплексный подход к защите компании от вредоносного кода // "Документальная электросвязь", №19, 2008
- **Сердюк В.А.** Комплексный подход к обеспечению безопасности на основе многоуровневой защиты от вирусных угроз // "Документальная электросвязь" №17, 2006
- **Сердюк В.А.** Комплексный подход к защите компании от угроз информационной безопасности // Презентация, ДиалогНаука, 2008
- **Калихман Р.** Forefront Client Security: технический обзор // Microsoft, слайды.
- **Косинов М.** Защита на уровне периметра сети: Microsoft ForeFront TMG и Microsoft Forefront IAG // **Softline**, слайды, 2009.
- **Трофимов А.** ForeFront TMG: обзор преемника ISA Server // Microsoft, слайды.


Спасибо за внимание!
Вопросы?