

# **Защита информации от современных угроз с помощью продуктов Лаборатории Касперского**



**Ипатов Илья**

Старший консультант  
службы консалтинга

# Современные ИТ угрозы

- **Вредоносное ПО**
- **Спам**
- **DoS атаки**
- **Фишинг**
- **Фарминг**
- **Блокинг**

# ФИШИНГ

The screenshot shows a SouthTrust Online Banking interface. At the top left is the SouthTrust logo. At the top right is a banner that says "Welcome to the Online Banking" with an image of a hand using a mouse. Below the banner is a navigation menu with items: "My Accounts", "Transfers & SouthTrust Bills", "Bill Payment", "User Preferences", "Customer Service", and "Help".

On the left side, there is a "My Accounts" sidebar menu with options: "Account Summary", "Transaction Search", "File Export", "Nicknames", "Add or Remove Accounts", "E-mail Notifications", and a "Logout" button.

The main content area contains the following text:

Required fields are marked with an \*.

\*Do you have a SouthTrust ATM Debit Card (This is required to confirm your identity as a card member of SouthTrust..)

Below this text is a form with the following fields:

Full Name:	<input type="text"/>
Bank Account Number:	<input type="text"/>
Credit/Debit Card Number:	<input type="text"/>
Cvv2 Code:	<input type="text"/>
Pin Number:	<input type="text"/>
Expiration Date:	<input type="text"/> <input type="text"/>

To the right of the form are two images of SouthTrust cards. The top one is a "CHECK CARD" (Visa) and the bottom one is an "ATM Debit Card" (Visa Plus Signature). Both cards have the name "ROBERT W. ANDREWS" and a card number. The ATM Debit Card number has a red box around the last four digits "0000".

At the bottom center of the form area is a "Continue" button.

# Фарминг

```
C:\ редактирование hosts4 - Far
D:\_new\!\Pharming\hosts4
72.9.232.244 www.bankone.com
72.9.232.244 bankone.com
72.9.232.244 halifax.com
72.9.232.244 www.halifax.com
72.9.232.244 halifax.co.uk
72.9.232.244 www.halifax.co.uk
72.9.232.244 www.bankofamerika.com
72.9.232.244 bankofamerika.com
72.9.232.244 www.paypal.com
72.9.232.244 paypal.com
72.9.232.244 www.lloydstsb.com
72.9.232.244 lloydstsb.com
72.9.232.244 www.lloydstsb.co.uk
```

# Блокинг

```
C:\ редактирование hosts4 - Far
D:\_new\!\Pharming\hosts4
127.0.0.1 www.kaspersky.com
127.0.0.1 www.kaspersky.ru
127.0.0.1 kaspersky.ru
127.0.0.1 www.kaspersky-labs.com
127.0.0.1 www.mcafee.com
127.0.0.1 www.mcafee.com
127.0.0.1 www.my-etrust.com
127.0.0.1 www.my-etrust.com
127.0.0.1 www.nai.com
127.0.0.1 www.nai.com
127.0.0.1 www.networkassociates.com
127.0.0.1 www.networkassociates.com
127.0.0.1 www.sophos.com
127.0.0.1 www.sophos.com
127.0.0.1 www.symantec.com
127.0.0.1 www.symantec.com
127.0.0.1 www.trendmicro.com
127.0.0.1 www.trendmicro.com
127.0.0.1 www.viruslist.com
127.0.0.1 www.viruslist.ru
127.0.0.1 www3.ca.com
```

## **Пути проникновения:**

- **Почта (70 - 80% вирусов)**
- **Интернет (10-15% вирусов)**
- **Конечные пользователи (5-10 %)**

## Поговорим о...

- защите Linux
- защите Check Point
- защите Novell
- защите Windows
- **Новинка** от  
Лаборатории Касперского

**NEW!!!**



# Защита Linux

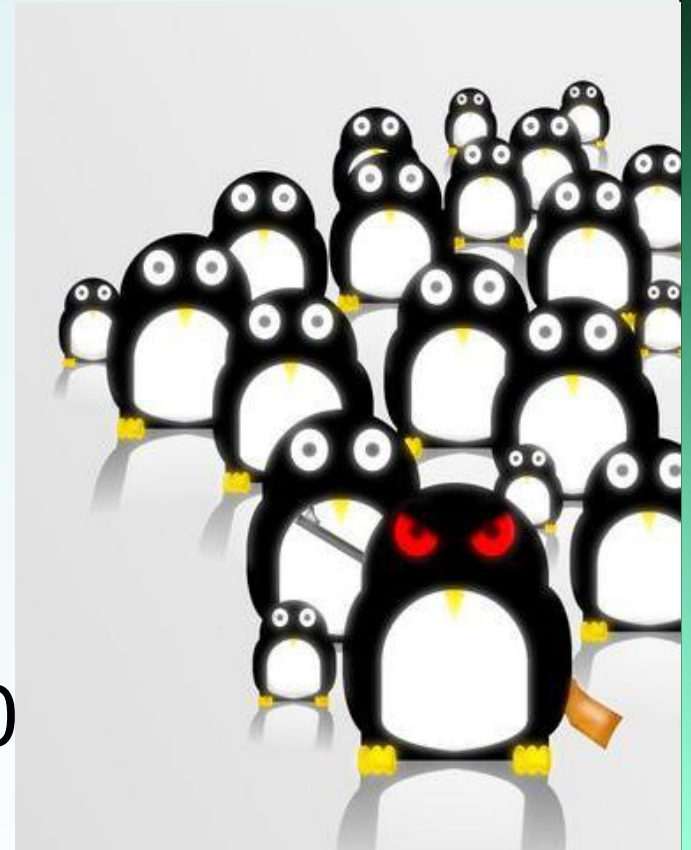




# Есть ли вирусы для Linux?

## Вирусы:

- для Linux ~ 986
- для Windows ~ 20000



# Что мы защищаем?

- Linux распространён на серверах – воротах в Интернет
- Linux надёжная и безопасная платформа для построения АВ решений
- Защита всей инфраструктуры, а не Linux

# Лаборатория Касперского и Linux

- ЛК была **первой** компаний которая предложила АВ решение для Linux
- ЛК занимается разработкой АВ продуктов для **Linux с 1999 года**
- ЛК предлагает законченное решение для Linux - **Kaspersky Linux Security**

# Kaspersky Linux Security

## Защита почты

KAV for Linux Mail Server  
Kaspersky Mail Gateway  
Kaspersky Anti-Spam



## Защита файл хранилищ

KAV for Linux File Server  
KAV for Linux Workstation



## Защита web трафика

KAV for Proxy Server



# Защита электронной почты

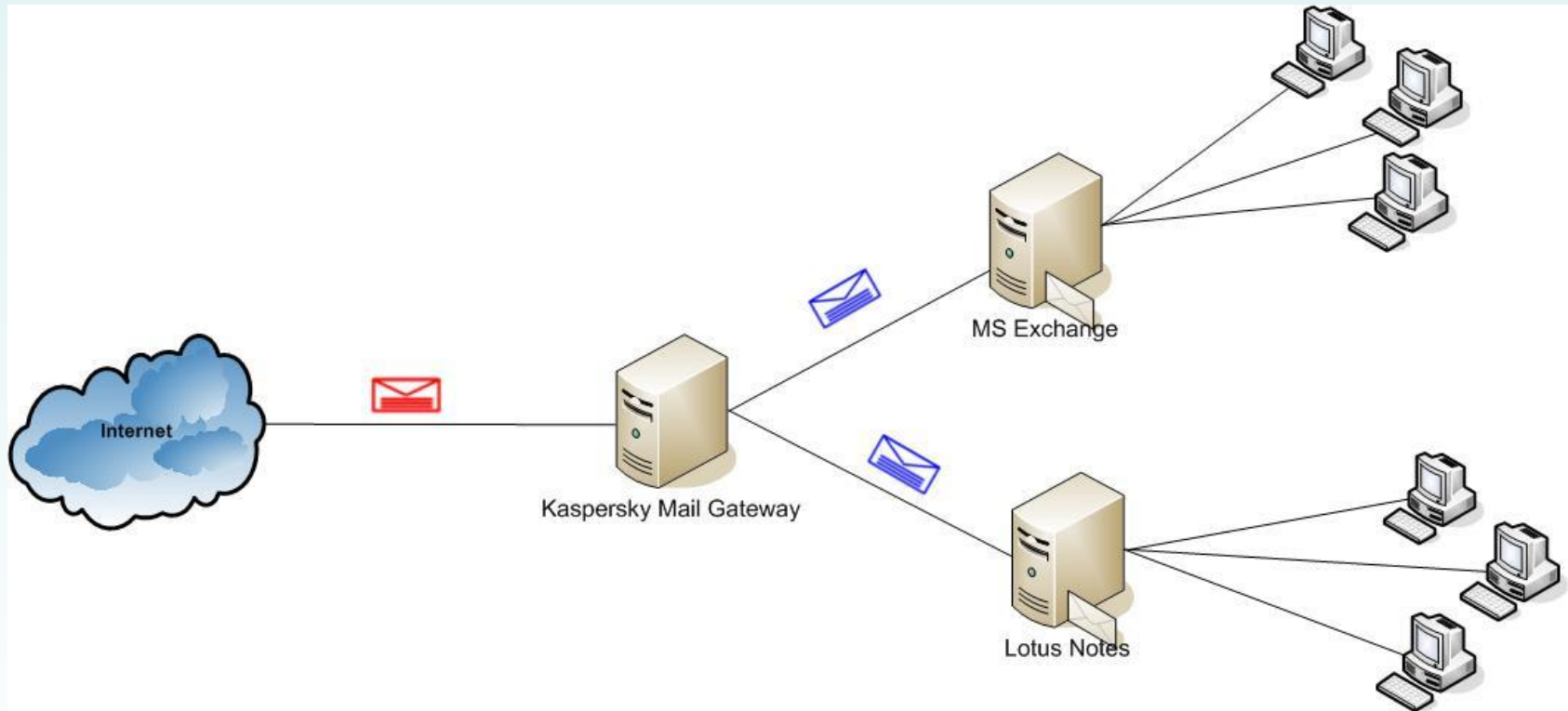
- Kaspersky Mail Gateway
- KAV for Linux Mail Server
- Kaspersky Anti-Spam



# Kaspersky Mail Gateway

- Защищает почтовый трафик от вредоносного кода и спама
- Легко интегрируется в любую сеть
- Не требует переконфигурации существующей почтовой системы

# Kaspersky Mail Gateway





# Преимущества решения

- Повышение уровня безопасности
- Упрощение администрирования
- Разделение нагрузки на почтовую систему

# Защита электронной почты

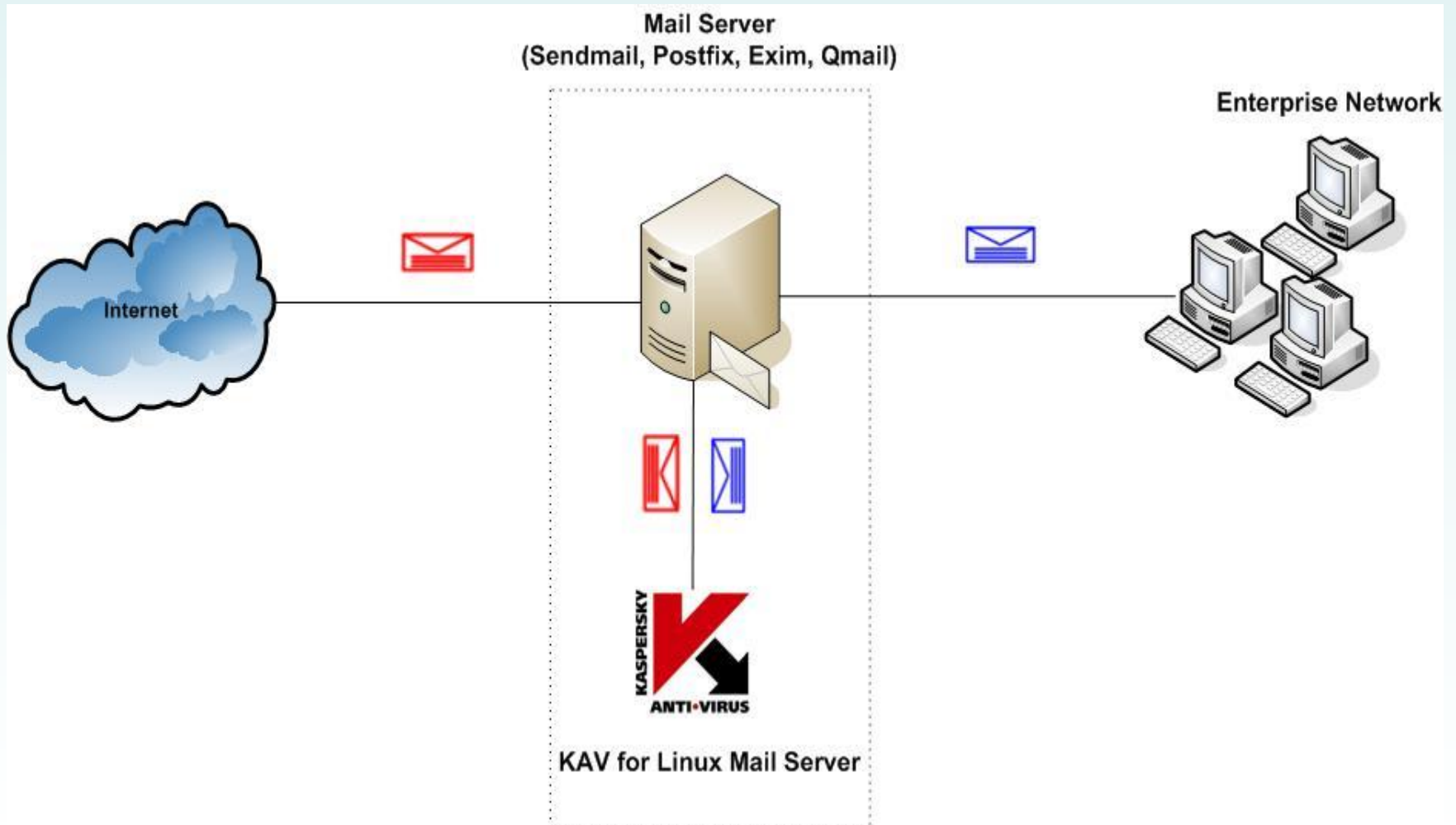
- Kaspersky Mail Gateway
- KAV for Linux Mail Server
- Kaspersky Anti-Spam



# **KAV for Linux Mail Server**

- Защищает почтовый трафик от вредоносного кода
- Интегрируется со следующими MTA:
  - **Sendmail**
  - **Postfix**
  - **Exim**
  - **Qmail**
- Карантин для инфицированных объектов
- Создание резервных копий перед лечением

# KAV for Linux Mail Server



# Защита электронной почты

- Kaspersky Mail Gateway
- KAV for Linux Mail Server
- Kaspersky Anti-Spam



# Kaspersky Anti-Spam 3.0



# Производительность и надежность

- Объем обновлений уменьшен в 3,5 раза
- Производительность выросла в 4,5 раза
- Обработка более 2.5 млн. сообщений в день на недорогом сервере: P4-2.6 / 1Gb RAM
- Проверено высокими нагрузками: фильтрует до 70 млн. сообщений в день на @Mail.Ru



# Защита web трафика

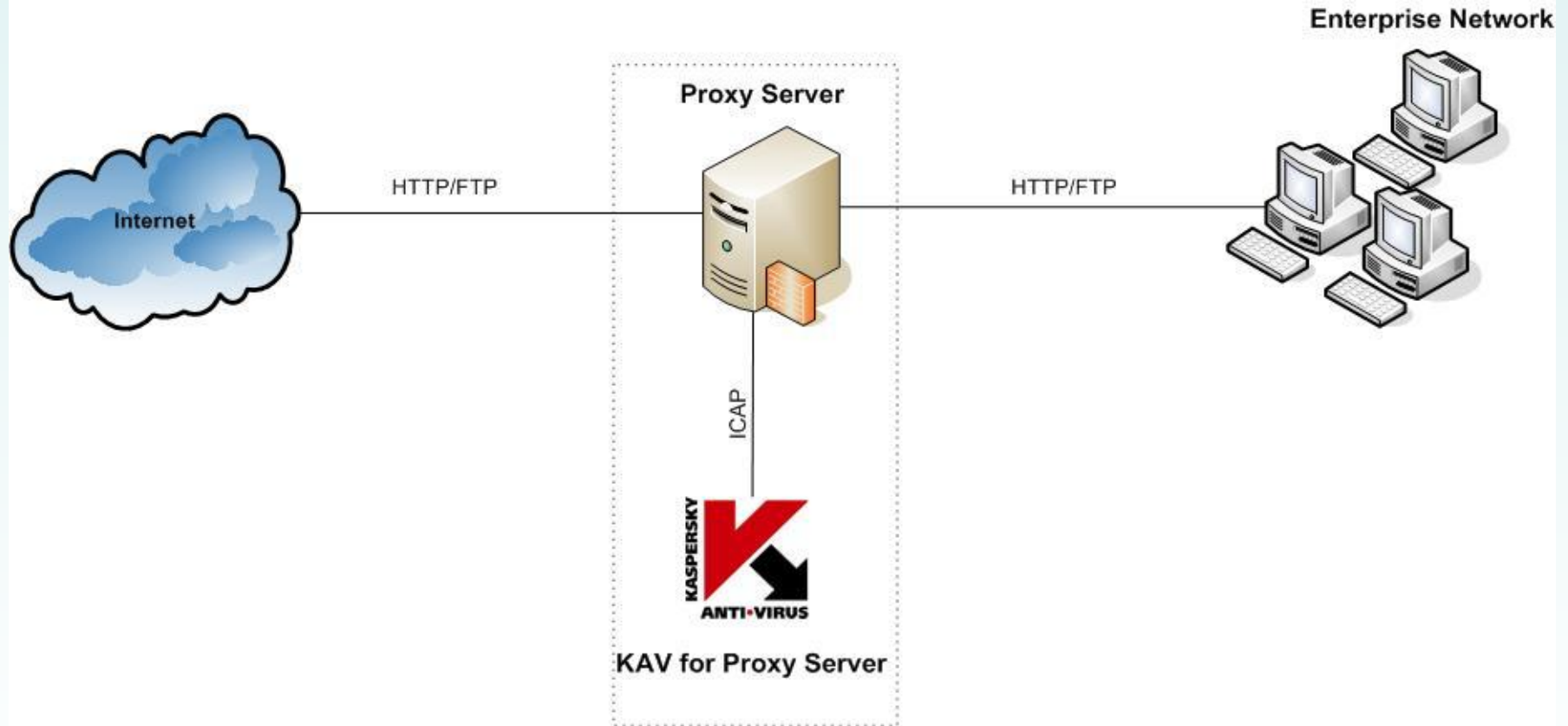
## KAV for Proxy Server



# KAV for Proxy Server

- Защищает web трафик от вредоносного кода в реальном времени
- Уведомляет пользователей о попытке скачать опасный объект
- Работает по протоколу ICAP
- Тестировался со Squid 2.5 (ICAP) и Squid 3.0 Pre Release
- Следующий MP поддержка:
  - BlueCoat SG
  - Cisco Content Engines

# KAV for Proxy Server



# Защита файловых серверов и рабочих станций

- KAV for Linux File Server
- KAV for Samba Server
- KAV for Linux Workstation



# **KAV for Linux File Server**

- Защищает систему в реальном времени
- Осуществляет проверку системы по требованию
- Модуль для защиты файловых хранилищ Samba в реальном времени
- Карантин для инфицированных объектов
- Создание резервных копий перед лечением

# Поддерживаемые платформы



# Kaspersky Linux Security Portal

## [www.kaspersky.ru/linux](http://www.kaspersky.ru/linux)

- Структурированная и полная информация о продуктах для Linux в одном месте
- Продуктовые листовки
- Истории успешных внедрений
- Документация
- Пробные версии продуктов
- Форма обратной связи с пользователями



# Защита для Check Point

## Антивирус Касперского 5.5 для Check Point Firewall-1



# В чём привлекательность?

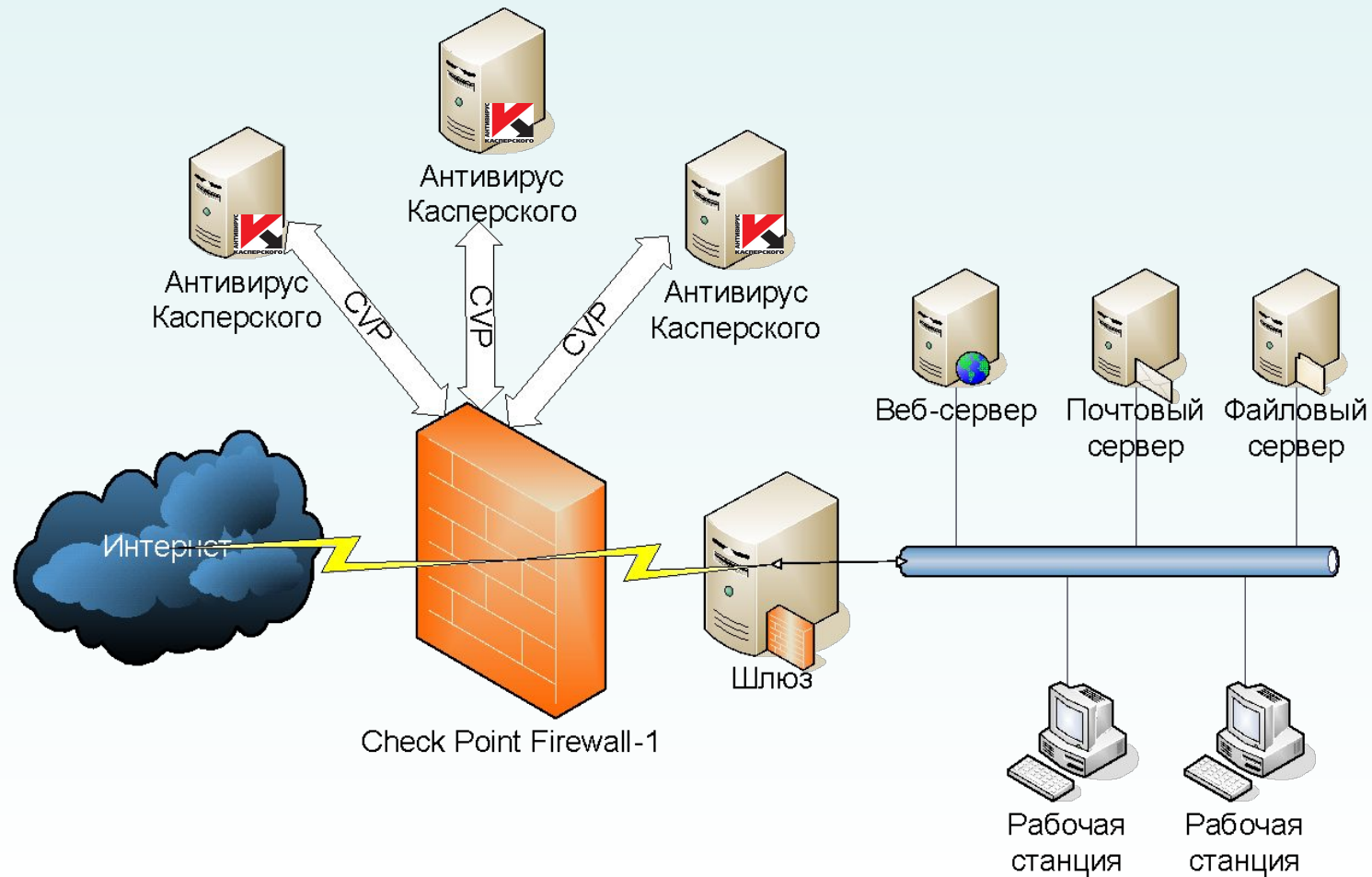
- Качественная защита информационных ресурсов организации от вредоносного ПО
- Невысокие издержки при реализации решения
- Невысокая общая стоимость владения
- Удобство администрирования приложения и обновления антивирусных баз
- Масштабируемость решения
- Поддержка современных аппаратных платформ

## **Производительность и масштабируемость решения**

- Проверка объектов «на лету».
- Возможность использования нескольких экземпляров Антивируса Касперского на нескольких физических серверах.
- Возможность запуска нескольких экземпляров антивирусного ядра.
- Настройка длины очереди проверяемых объектов.

**Наше решение быстрее, чем протокол CVR**

# Интеграция



# Защита файловых серверов и серверов приложений Novell

KAV for Novell Netware 5.6



# **Основные возможности**

## **Антивирусная функциональность**

- Постоянная защита файлового сервера с возможностью лечения, переименования, удаления зараженных объектов.
- Возможность блокирования соединения с рабочей станцией, откуда производилась попытка доступа к зараженному объекту
- Проверка сервера по требованию позволяет одновременно запускать несколько задач сканирования с различными настройками по расписанию или по команде администратора
- Проверка файлов не только при создании и открытии, но и при изменении
- Автоматическое обновление антивирусных баз по расписанию или по требованию администратора

# Защита Windows





# Защита почты

- **Kaspersky Security 5.5** for Microsoft Exchange Server 2003
- **Kaspersky Anti-Virus 5.5** для MS Exchange Server 2000\2003

# Продукты Лаборатории Касперского для защиты MS Exchange Server

- Kaspersky Security 5.5 for Microsoft Exchange Server 2003
  - Антивирусный модуль
  - **Анти-Спам модуль**
  
- Kaspersky Anti-Virus 5.5 для MS Exchange Server 2000\2003
  - Антивирусный модуль

## Kaspersky Security 5.5 for Microsoft Exchange Server 2003

- Продукт объединяет:
  - Kaspersky Anti-Virus 5.5
  - Kaspersky Anti-Spam 2.0 (портированный на Windows)
- Поддержка инфраструктуры [Microsoft Spam Confidence Level](#), встроенной в Microsoft Exchange Server 2003
- Настройка обновлений:
  - Антивирусных баз – 1 раз в час
  - Антиспам-баз – каждые 20 минут
- Интеграция с Kaspersky Administration Kit
- Работа в массивах серверов

## Преимущества решения:

- Комплексное решение для защиты от вирусов и спама
- Использование передовых технологий
- Двухуровневая фильтрация спама
- Невысокая общая стоимость владения
- Поддержка кластерной технологии
- Масштабируемость / производительность
- Тонкая настройка приложения
- Простота установки и быстрое начало работы

## Качество распознавания спама

- Крайне низкий уровень ложных срабатываний – около 0,001% (1 письмо на 10 000 сообщений)
- Уровень фильтрации спама – до 98%

# Защита HTTP и FTP трафика

**KAV for Microsoft ISA Server**

2000/2004 Enterprise Edition



## Преимущества решения:

- Надежная защита от вирусов и вредоносного кода
- Экономичность использования
- Удобство управления
- Оптимизация нагрузки на сервер
- Простота установки

## **Ближайшие перспективы**

- Отчеты о результатах антивирусной защиты по: клиенту, сайту, разновидности вируса.
- Проверка исходящего SMTP и входящего POP3 потока данных, проходящего через Microsoft ISA Server
- Резервное хранилище для обнаруженных в SMTP, POP3 потоке инфицированных почтовых сообщений.



# Защита рабочих станций

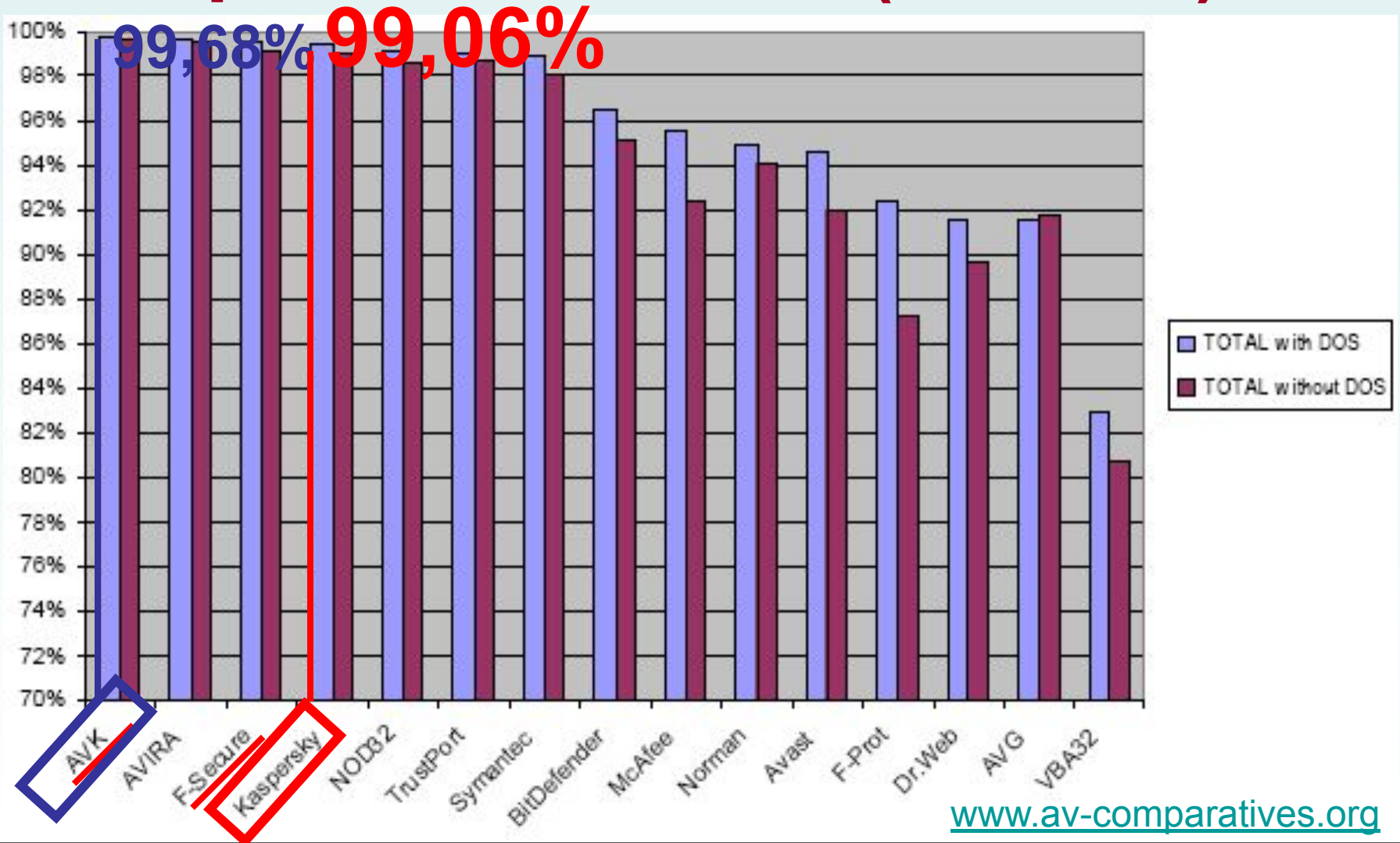
## KAV for Windows Workstations



# Миф

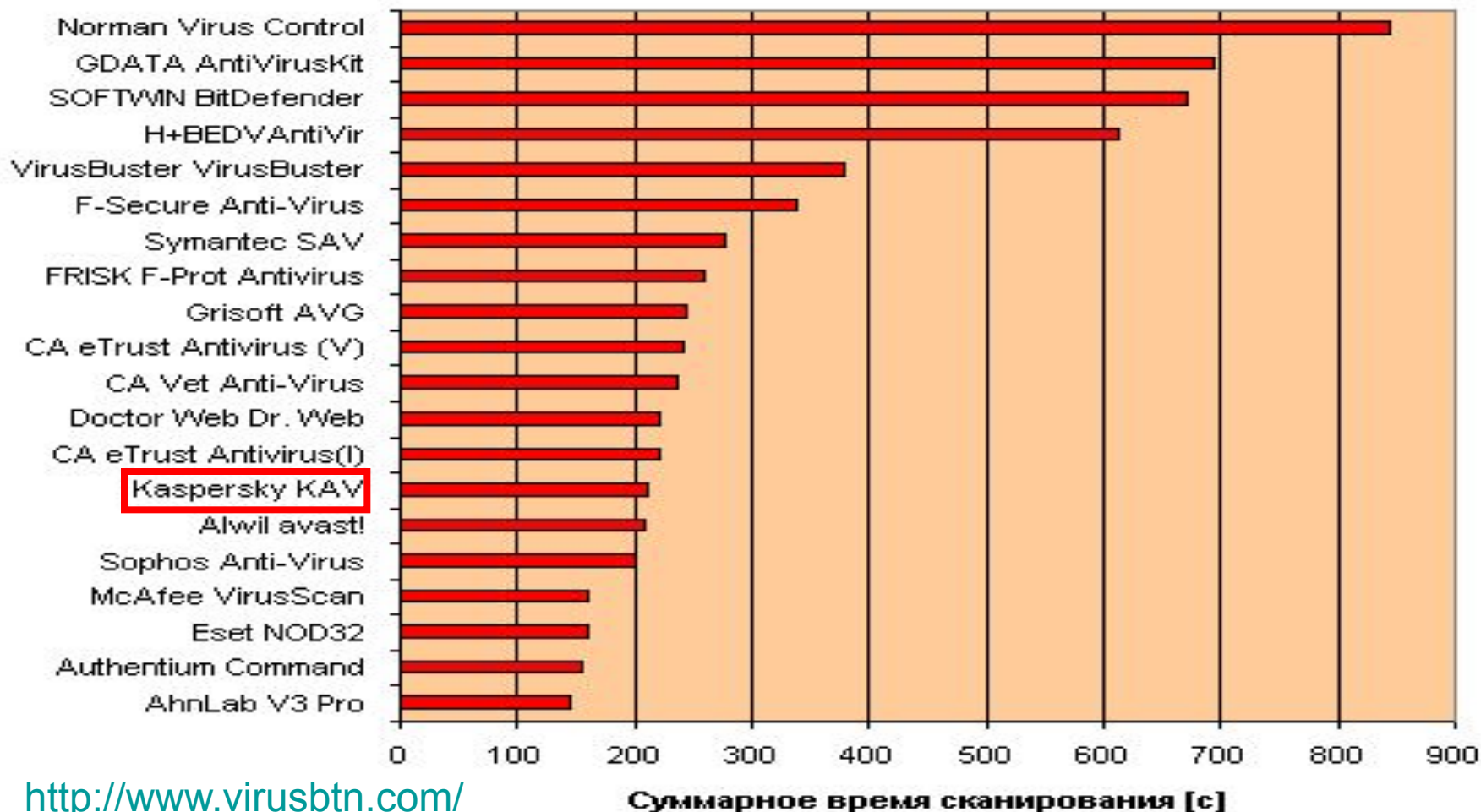
**Касперский тормозит систему!**

# Уровень детекта (551 795)



# Скорость сканирования

Общая скорость сканирования



# Майк

При отличном уровне детекта,  
Касперский тормозит систему  
меньше других антивирусов!

# Антивирус Касперского для рабочих станций Windows 6.0

## Что нового.....?

- Компонентная структура
- Комплексная защита от всех видов вредоносных программ
- Качество детектирования
- Скорость работы
- Пользовательский интерфейс

# **Защита от всех видов компьютерных угроз**

- **Файловый антивирус**
- **Почтовый антивирус**
- **Веб-Антивирус**
- **Проактивная защита**
- **Анти-Шпион**
- **Анти-Хакер**
- **Анти-Спам**
- **Мастер создания диска аварийного  
восстановления**



# Скорость работы

- Технологии iSwift и iChecker
- Приостановка сканирования
- Технология SafeStream
- Компактные обновления
- Сетевой iSwift

# Сравнение функционала

Компоненты защиты	5.0	6.0
Файловый антивирус	■	■
Почтовый антивирус	■	■
Веб-Антивирус		■
Проактивная защита		■
Анти-Хакер		■
Анти-Шпион		■
Анти-Спам		■

**Цена останется неизменной**

# Защита файловых серверов

## KAV for Windows Fileserver



# Новые технологии

- Несколько экземпляров антивирусного ядра
- Распределение нагрузки на процессоры сервера
- Изоляция зараженных компьютеров
- Четыре режима окончания сканирования
- Гибкая настройка времени сканирования
- Настройка уведомлений

# Централизованное управление КСАЗ

## Kaspersky Administration Kit



## Что нового?

- Дополнительные плагины управления
- Удаление сторонних антивирусных продуктов
- Поддержка IP multicasts
- Создание резервной копии
- Расширенный мониторинг
- Добавлен узел «Резервное хранилище»

**Скачать бета-версию**

**[www.kaspersky.ru/beta](http://www.kaspersky.ru/beta)**

# Kaspersky® Hosted Security mailDefender

АБСОЛЮТНО НОВОЕ  
РЕШЕНИЕ ПО ЗАЩИТЕ  
КОРПОРАТИВНОЙ ПОЧТЫ

Комплексное решение задачи

защиты почтовых потоков

предприятий

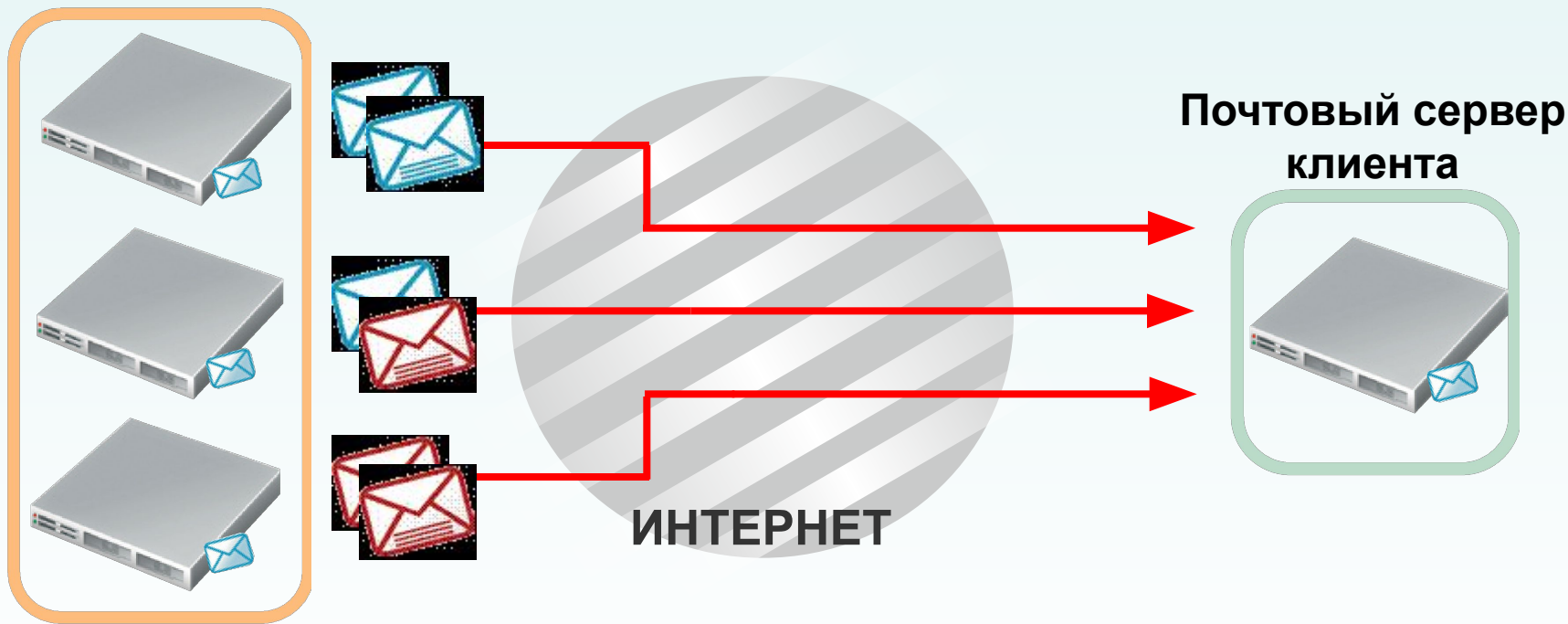


# Что такое mailDefend

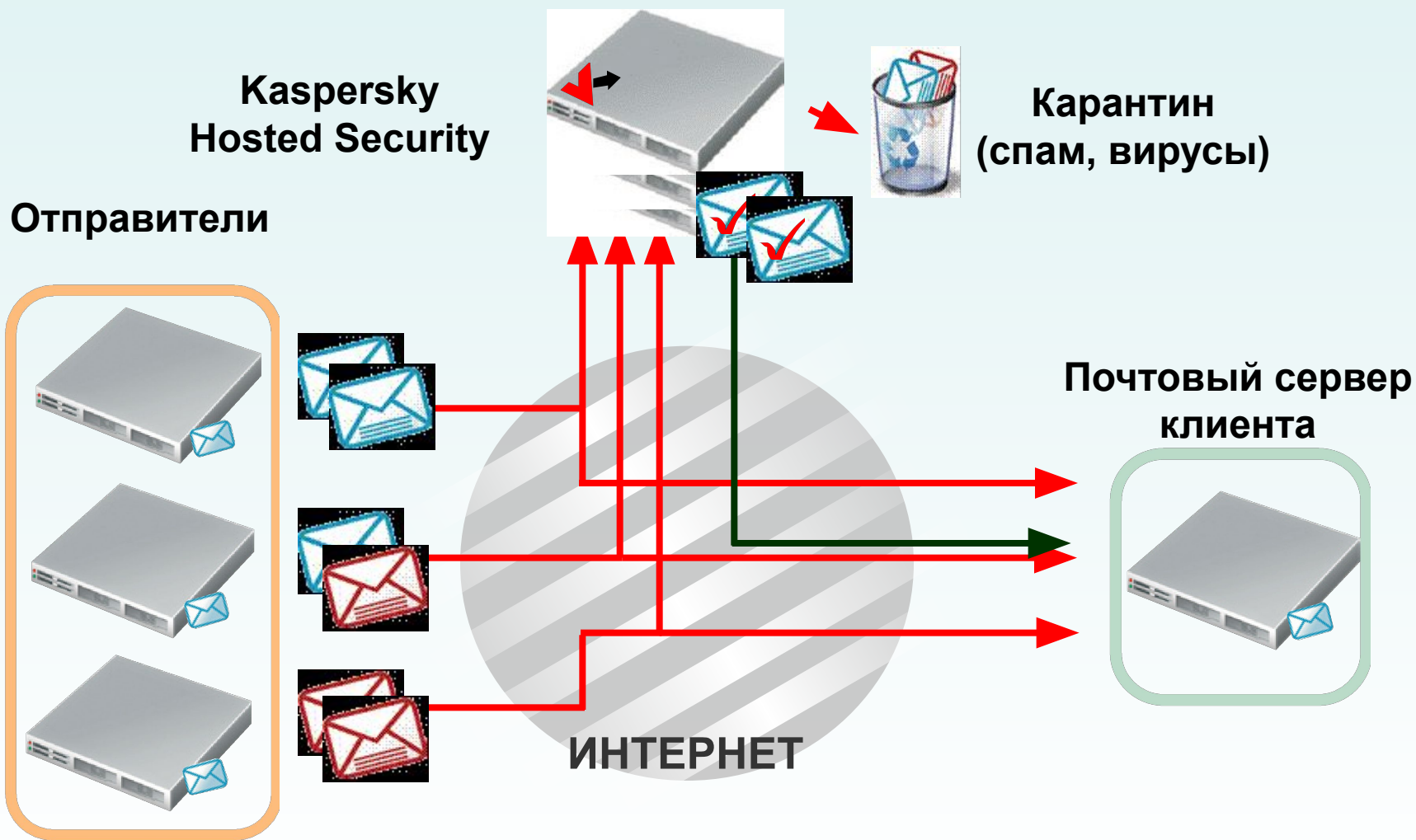
- Защита электронной почты
- Не требует приобретения дополнительного программного или аппаратного обеспечения
- Развёртывание за несколько минут
- Не требует установки какого-либо программного обеспечения на почтовый сервер.
- Масштабируется вместе с ростом вашей компании
- Постоянно развивается с тем, чтобы противостоять изменяющимся Internet угрозам.
- Совместимость с любым почтовым сервером

# Обычный путь почты

Отправители



# mailDefend

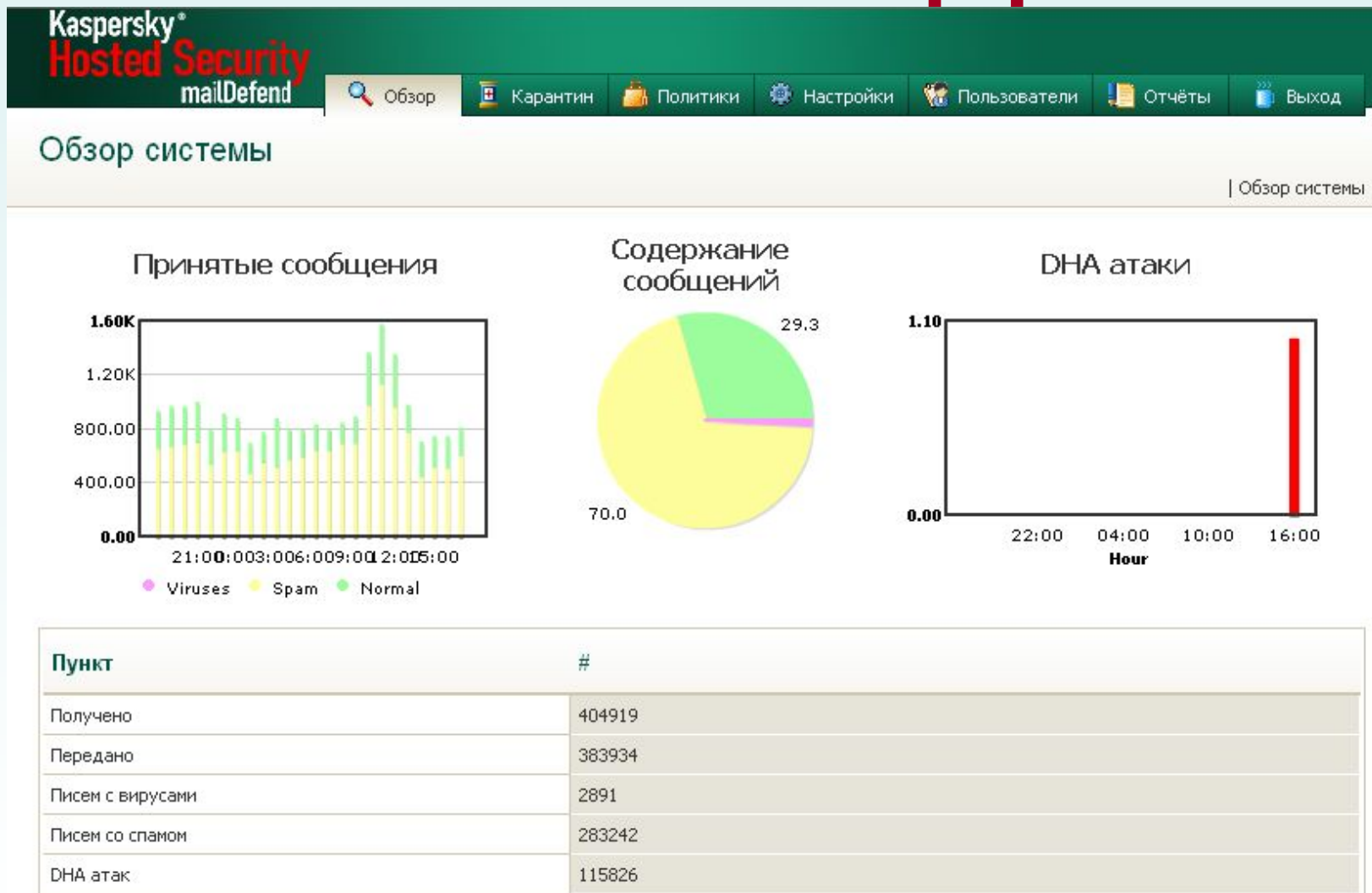


## **mailDefend: основные элементы**

- Антивирус
- Антиспам
- Политики безопасности
- Отказоустойчивость
- Система управления



# mailDefend: интерфейс



# Служба консалтинга ЛК

## Плановые работы (в штатном режиме):

- Полный спектр работ, связанных с созданием комплексных систем антивирусной защиты (КСАЗ) корпоративных ИТ-инфраструктур
  - Проведение аудита антивирусной защиты корпоративных систем
  - Анализ состояния антивирусной защиты и выработка рекомендаций
  - Создание/модернизация КСАЗ «под ключ», разработка методик тестирования/внедрения/модернизации САЗ
  - Создание руководящих документов по эксплуатации САЗ
  - Выработка политик антивирусной защиты предприятий
  - ...

## Работы в режиме «ЧС»

- Анализ ситуаций, возможно вызванных проникновением вредоносных программ, их выявление и помощь в устранении

# Сервис для пользователей

- возможность получения **ежедневных обновлений** антивирусных баз по электронной почте;
- предоставление **новых версий** программного приложения;
- консультации по вопросам, связанным с установкой, настройкой и эксплуатацией (**техподдержка**)
- оповещение о выходе **новых приложений** в Лаборатории Касперского и о **новых вирусах**, появляющихся в мире

**Вопросы?**



**Спасибо за внимание.**

