Глава 01
Что такое спам

История спама

- **1978**
  - первая рассылка по e-mail
- **1994**
  - первая рекламная рассылка в сети Usenet
- **1996-1998**
  - массовое распространение спама
  - более 50% всей почты - спам
- **1997**
  - появление средств для борьбы со спамом (DNSBL, SpamAssassin.org)
- **Наши дни**
  - спам во всех областях электронных коммуникаций

Что такое спам?

- Спам - рассылка сообщений по электронной почте
  - Незапрошенная
  - Массовая
  - Анонимная

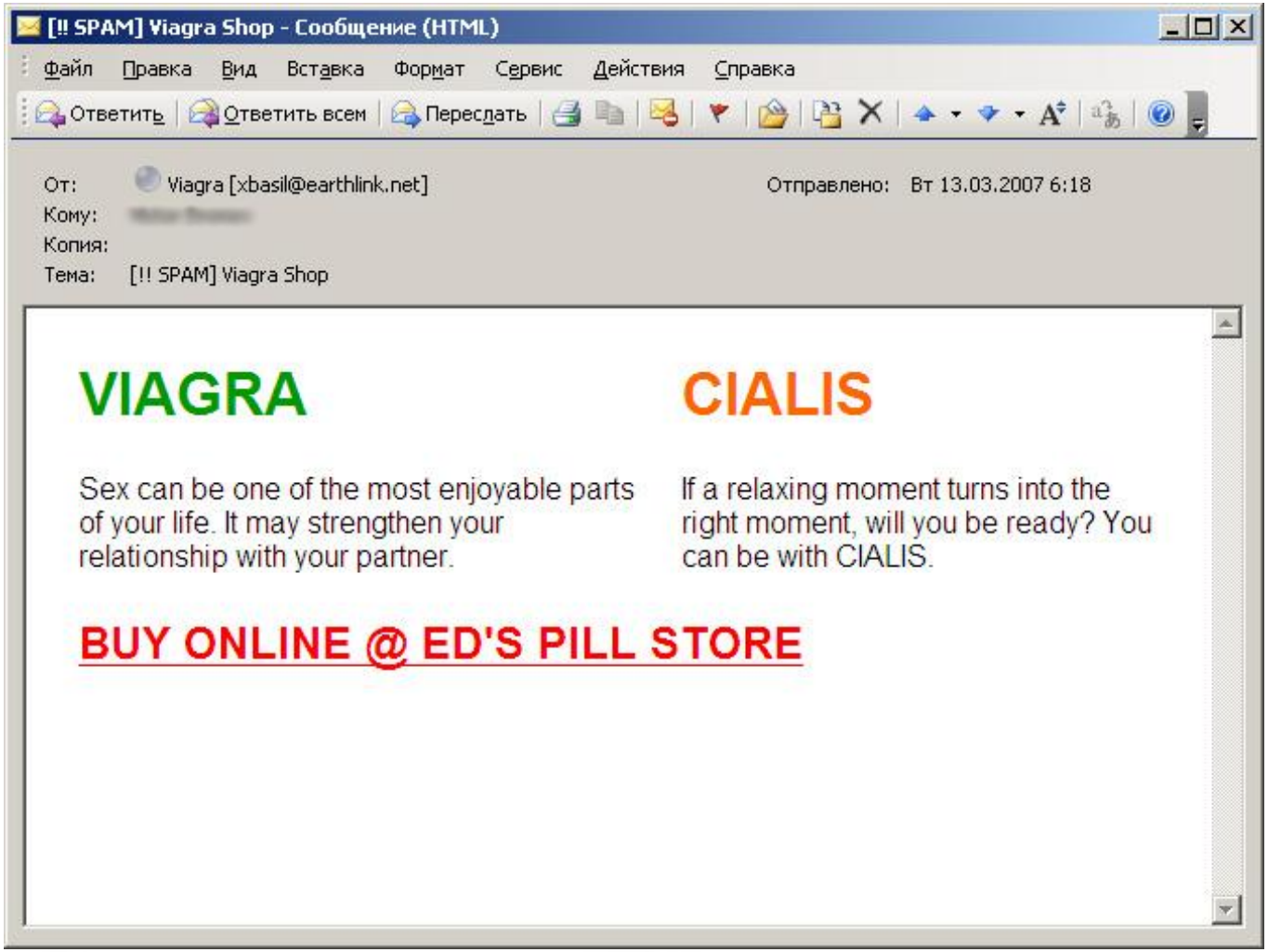
Что НЕ является спамом?

- Регулярные подписные рассылки
- Автоматические ответы серверов
- Рассылки «вручную» от менеджеров по продажам
- Просто «нежелательные» сообщения

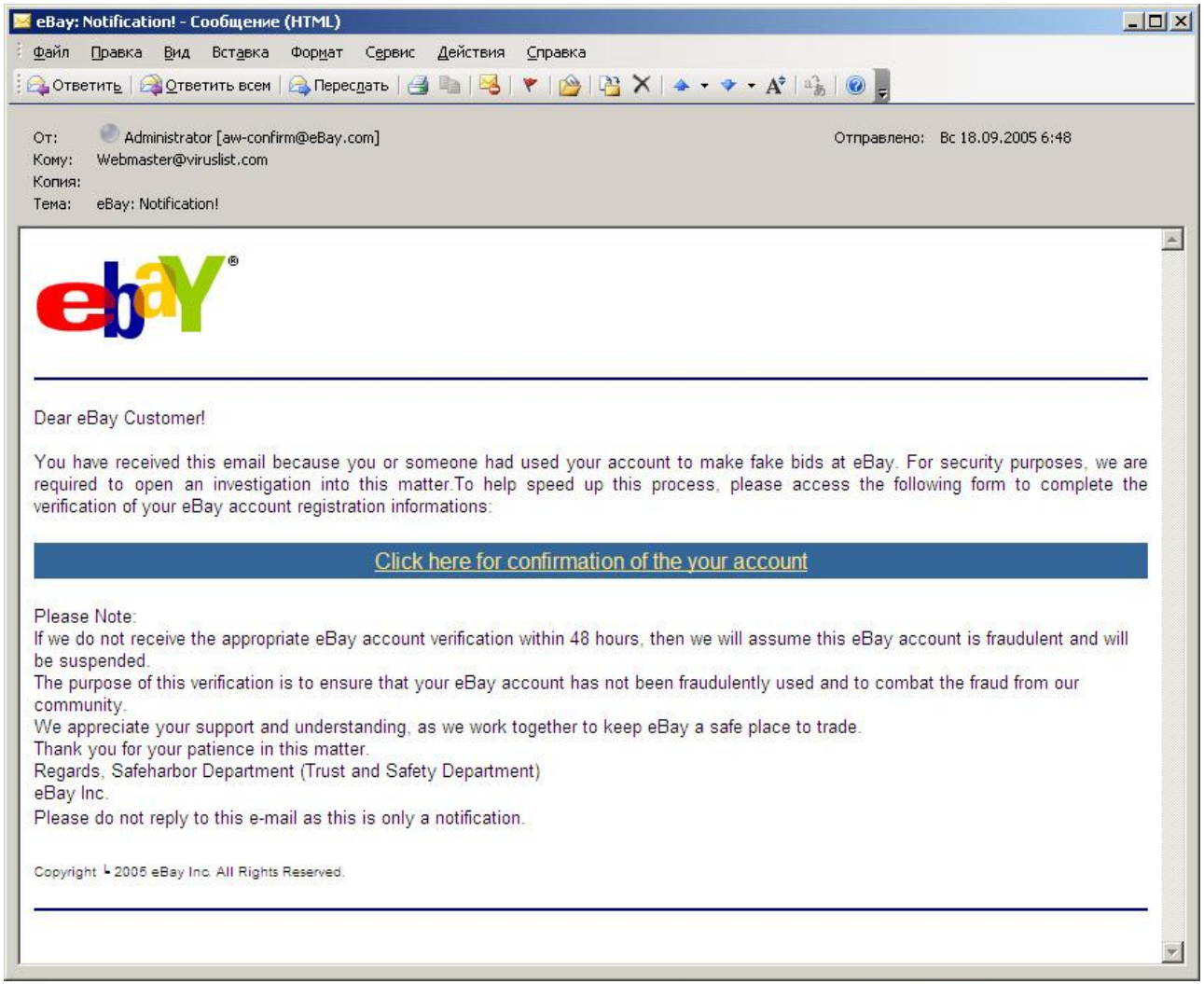
Цели рассылки спама

- Реклама
- Мошенничество
  - фишинг
  - «нигерийские письма»
- Рассылка вредоносного ПО
- Черный PR, игра на бирже
- Политическая агитация

Пример рекламного спама



Пример фишинга



eBay: Notification! - Сообщение (HTML)

Файл Правка Вид Вставка Формат Сервис Действия Справка

Ответить | Ответить всем | Переслать

От: Administrator [aw-confirm@eBay.com]
Кому: Webmaster@viruslist.com
Копия:
Тема: eBay: Notification!
Отправлено: Вс 18.09.2005 6:48

Dear eBay Customer!

You have received this email because you or someone had used your account to make fake bids at eBay. For security purposes, we are required to open an investigation into this matter.To help speed up this process, please access the following form to complete the verification of your eBay account registration informations:

Click here for confirmation of the your account

Please Note:
If we do not receive the appropriate eBay account verification within 48 hours, then we will assume this eBay account is fraudulent and will be suspended.
The purpose of this verification is to ensure that your eBay account has not been fraudulently used and to combat the fraud from our community.
We appreciate your support and understanding, as we work together to keep eBay a safe place to trade.
Thank you for your patience in this matter.
Regards, Safeharbor Department (Trust and Safety Department)
eBay Inc.
Please do not reply to this e-mail as this is only a notification.

Copyright © 2005 eBay Inc. All Rights Reserved.

Пример «биржевого» спама

WATCH OUT!
HERE COMES THE BIG ONE!
WEDNESDAY AUG 23rd IS SURE TO BE A BIG DAY!

Company Name: WILD BRUSH ENERGY (Other OTC:WBRS.PK)
Symbol: WBRS
1-day Target: 0.2

WILD BRUSH MAKES A MOVE!
Wild Brush Acquires Additional Powder River Oil _Gas Lease.
Read More Online NOW!

Who is Wild Brush?

Wild Brush Energy is a diversified energy company whose primary goal is to identify and develop
Oil _Coalbed Methane sites within the State of Wyoming.
In addition, Wild Brush Energy continues to evaluate clean air alternative energy producing technologies such as Wind Power.
Wild Brush trades in the U.S. under the symbol "WBRS."

Currently trading in the .05 range! Now is your chance!
ADD THIS GEM TO YOUR WATCH LIST, AND WATCH IT TRADE CLOSELY ON WEDNESDAY AUGUST 23rd!

Спам – это выгодно

- Дешевый контакт с получателем для рекламодателя
- Доходы от рекламы для спамера
- Продажа/использование похищенных банковских данных
- Косвенные доходы от спама
  - при игре на бирже
  - агитации
  - PR и т.д.

Ущерб от спама

- Потеря времени сотрудников
  - до 2% общего рабочего времени
- Затраты времени ИТ-персонала
  - до 50% при работе с почтовыми системами
- Инвестиции в ИТ-инфраструктуру
  - до 90% нагрузки на сервера - спам
- Увеличение интернет-трафика
  - 70-90% всего почтового трафика - спам
- Риск вирусных атак и фишинга в спаме

Глава 02
Технологии рассылки спама

Прямая рассылка

- Используется небольшими компаниями
- Не используются специфические технологии отправки и обхода спам-фильтров
- Используется собственный виртуальный или физический почтовый сервер
- Легко идентифицируется и блокируется ISP

Рассылка с выделенного сервера

- Аренда или установка сервера у провайдера
- Прямая рассылка (с выделенного сервера)
- Легко идентифицируется ISP…
  - …если ISP хочет это идентифицировать

Рассылка через dial-up провайдеров

- Дешевый, быстрый, анонимный спам
- Норма
  - отправка через сервер провайдера
- Уловка
  - отправка напрямую получателю

- Способ борьбы
  - Dial-Up Users List (DUL)

Использование открытых релеев (Open Relay)

- Что такое открытый релей?
- Бесплатно и анонимно
  - чужой сервер
  - чужой IP
- Борьба с открытыми релеями, «черные списки»

Использование зомби-сетей

- Самый распространенный способ рассылки
- Самый технически сложный способ рассылки
- Тесная интеграция с вирусным сообществом
- Принцип работы зомби-сети
  - Заражение ПК
  - Получение команды от Управляющего Центра
  - Рассылка спама незаметно для владельца ПК

Особенности работы зомби-сетей

- «Быстрая и глупая» сеть
  - рост скоростей рассылки с появлением зомби-сетей
- «Медленная, но умная» сеть
  - усложнение технологий рассылки

- Сложности в борьбе с зомби-сетями
  - динамический состав зомби-сетей
    - нельзя заблокировать по IP на 100%
  - устойчивость зомби-сетей
    - нельзя «выключить» как открытый релей или сервер

Длительность рассылки

- Дни
  - Прямая рассылка
  - Dial-up аккаунты
  - Открытые релеи
- Часы
  - Собственный сервер на площадке провайдера
  - «Медленные» зомби-сети
- Менее часа
  - «Быстрые» зомби-сети

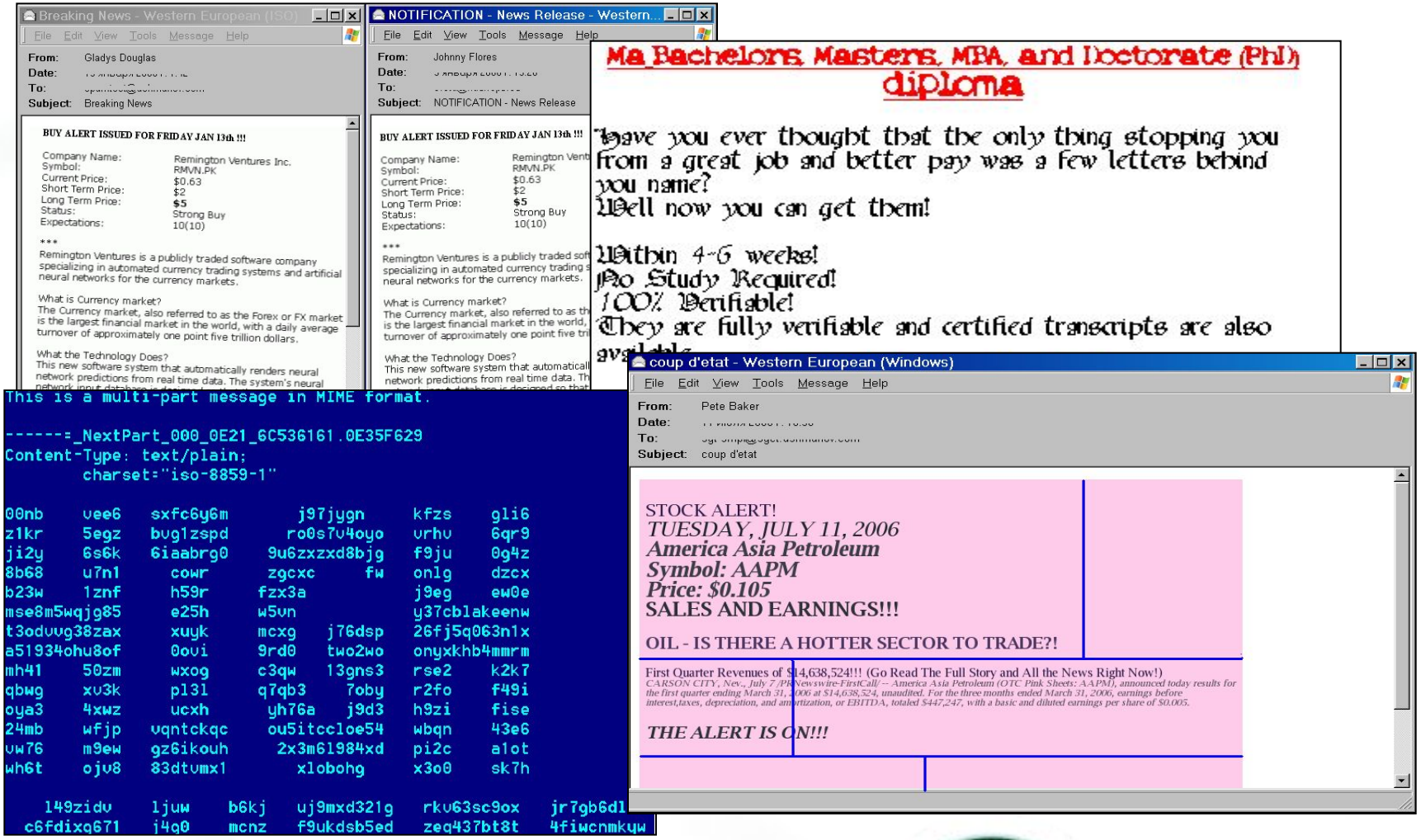
Базы адресов для рассылки

- Программы-роботы
  - поиск адресов на веб-страницах
  - в форумах
  - блогах и т.д.
- Продажа спамерам баз email-адресов своих клиентов нечистыми на руку компаниями
- Генерация случайных имен и использование словарей наиболее популярных имен (info@, sales@, john@ и т.д.)

Приемы для обмана спам-фильтров

- Подмена адреса отправителя
- Искажения текста: V!A_GrA
- Мусорный текст – в конце письма, белый на белом и др.
- Спам в картинках
- Анимированный спам
- … множество других способов

Примеры графического спама



Анимированный спам: отдельные кадры

BullsEye Financial Weekly Report September Issue:

Make no mistake, our mission at BullsEye Financial is to sift through the thousands of underperforming companies out there to find the golden needle in the haystack.

The micro-cap diamond that can make you a fortune. More often than not, the stocks we profile show a significant increase in stock price, sometimes in days or hours, not months or years.

We have come across what we feel is one of those rare deals that the public has not heard about yet.

Trade Date: Tuesday, September 5, 2006
Company : TRIMAX CORPORATION
Ticker : TMXO
Current Price : $0.38
Short Term Target Price : $1.50
Long Term Target Price : $2.50
Recommendation: STRONG BUY

Brokers and Day-Traders are gonna be scrambling Tuesday Morning.
Don't let them beat you to the punch, get in EARLY on Tuesday morning!!!
We all know that in the this business it's the big announcements that makes these explode!

Приемы социальной инженерии

- Социальная инженерия – методы манипулирования человеком для побуждения его к неким действиям.

- Применение в спаме
  - Фишинг
  - Нигерийские письма
  - «Биржевой спам»

Глава 03
Технологии борьбы со спамом

Основные методы борьбы

- Черные списки
  - IP адресов – DNSBL (RBL)
  - URL в теле письма – URIBL
- Greylisting
  - «серые» списки IP адресов
- Авторизация отправителя письма
  - SPF, Sender ID, DomainKeys
- Лингвистический и эвристический анализ
- Анализ массовости рассылок в Интернет
- Самообучаемые фильтры
  - Байес и др.

DNSBL (RBL)

RBL (торговая марка) – Real-time Blackhole List

- DNSBL – DNS Black List
  - Содержит базу данных IP с которых рассылается спам
  - «Срок жизни» IP в базе данных ограничен
- Виды DNSBL
  - Коммерческие, предоставляемые как сервис
  - Бесплатные, существующие как open source проекты
  - Собственные «черные списки» для собственных нужд

- Плюсы
  - бесплатность
  - экономия трафика
- Минусы
  - ложные срабатывания
  - сложность обнаружения ложных срабатываний

URIBL (URL BL)

- URI = URL = Uniform Resource Locator
- URIBL – база данных ссылок, рекламируемых в спаме
- SURBL.org – один из бесплатных сервисов

- Плюсы
  - точная работа
- Минусы
  - не дает всеобъемлющей картины

Grey listing

- Письмо с «нового» адреса не принимается, сервер дает отправителю команду «Повтори попытку позже»
- Легальный сервер выполнит команду, спамерский – повторит попытку сразу же
- На основании поведения сервера-отправителя письмо заносится в «черный» или «белый» список

SPF (а также SenderID, DomainKeys…)

- Подтверждают, что домен сервера-отправителя не подделан
- Требуют ряда действий от домена-отправителя для того, чтобы проверка могла работать
  - данные технологии поддерживают лишь 1-2% почтовых систем в Интернет
- Сами по себе не определяют спам, а дают лишь дополнительную информацию для анализа

Лингвистический анализ

- Ведение базы данных лексикона спама (вендор)
- Постоянное обновление базы данных (вендор)
- Автоматический анализ текста сообщения на основании частоты и характера употребления «спамерской» лексики в сообщении (спам-фильтр)

- Плюсы
  - при грамотной реализации – очень точно определяет спам
- Минусы
  - требует обновлений и быстрой реакции вендора
  - бессилен против графического спама

Анализ массовых рассылок

- Определяет спам на основании начала массовой рассылки одинаковых/схожих сообщений самым разным получателям
- Требует доступа к статистике крупных почтовых систем (например, Commtouch)

Обучающиеся алгоритмы (Байес и др.)

- Самый большой миф в области антиспама
- Обучение на «хороших» и «плохих» письмах

- Плюсы
  - не требует обновлений
- Минусы
  - несложно обмануть
  - требует активного участия пользователя

Эвристика

- Принцип, используемый во многих методах
  - эвристический анализ подразумевает начисление некоторых «баллов» письму, и затем – отнесение его к спаму (или нет) на основании суммы баллов
- Эвристика применяется в...
  - ...лингвистическом анализе (баллы за каждое «подозрительное» слово)
  - ...анализе технических параметров («конверта») письма: заголовков, полей From и To и т.д.
  - ...и самое главное – при комплексном подходе к фильтрации спама

Комплексный подход

- Один метод не может учесть все аспекты
- Каждый метод имеет свои преимущества
- Каждый метод имеет недостатки
- Все наиболее известные антиспам-продукты используют комплексный подход

Глава 04
Оценка эффективности антиспам-решений

Detection rate

- Показатель качества спам-фильтра №1
- DR = число детектированных спам-писем / число всех спам-писем в почтовом потоке
  - Пример
    - получено 110 писем, 100 из них спам
    - помечено как спам 90 писем… DR = ?
- DR невозможно вычислить автоматически

Уровень ложных срабатываний (FPR)

- Тоже показатель качества спам-фильтра №1
- FPR = число «чистых» писем, ошибочно помеченных как спам / число всех «чистых» писем
- FPR невозможно вычислить автоматически
- Важность показателя и маркетинговые уловки вендоров

«Быстрая» оценка эффективности решения

- Берем почтовые ящики куда приходит только спам (не менее 99% от всей приходящей почты)
- Фильтруем продуктом эти ящики, оцениваем долю почты, помеченной как спам
- Быстрый подход имеет свои недостатки
  - Не оценивается уровень ложных срабатываний
  - Тестирование менее 2 недель не всегда дает точные результаты
  - Наличие «специфики конкретного почтового ящика»

«Быстрое» сравнение продуктов

- Берем тот же источник «условного спама»
- Устанавливаем несколько альтернативных фильтров
- Подаем на вход каждому идентичный поток почты
- Сравниваем долю отсева почты для каждого
- Помним про те же минусы «быстрого» подхода

Полное тестирование

- Фильтрация
  - режим реального времени
- Длительность теста
  - не менее 2 недель
- Адресов для тестирования
  - не менее 20
- Аккуратнее с пересылкой в Windows
- Поставьте все фильтры в равные условия

Типичные ошибки при тестировании

- «Мне приходит много спама»
  - А сколько не приходит?
- «Почему фильтр не блокирует 100% спама?»
  - Потому что это невозможно
- «Мы протестировали на нашей спам-коллекции…»
  - Никаких спам-коллекций!

Типичные ошибки при тестировании

- «Доля спама всего 50% ..!»
  - Считаем detection rate, не долю
- «Фильтр установили, пользователям не сказали»
  - Пользователи должны знать как фильтруется их почта!
- «Фильтр А поймал то, что фильтр Б пропустил!»
  - Фильтры нельзя тестировать последовательно!

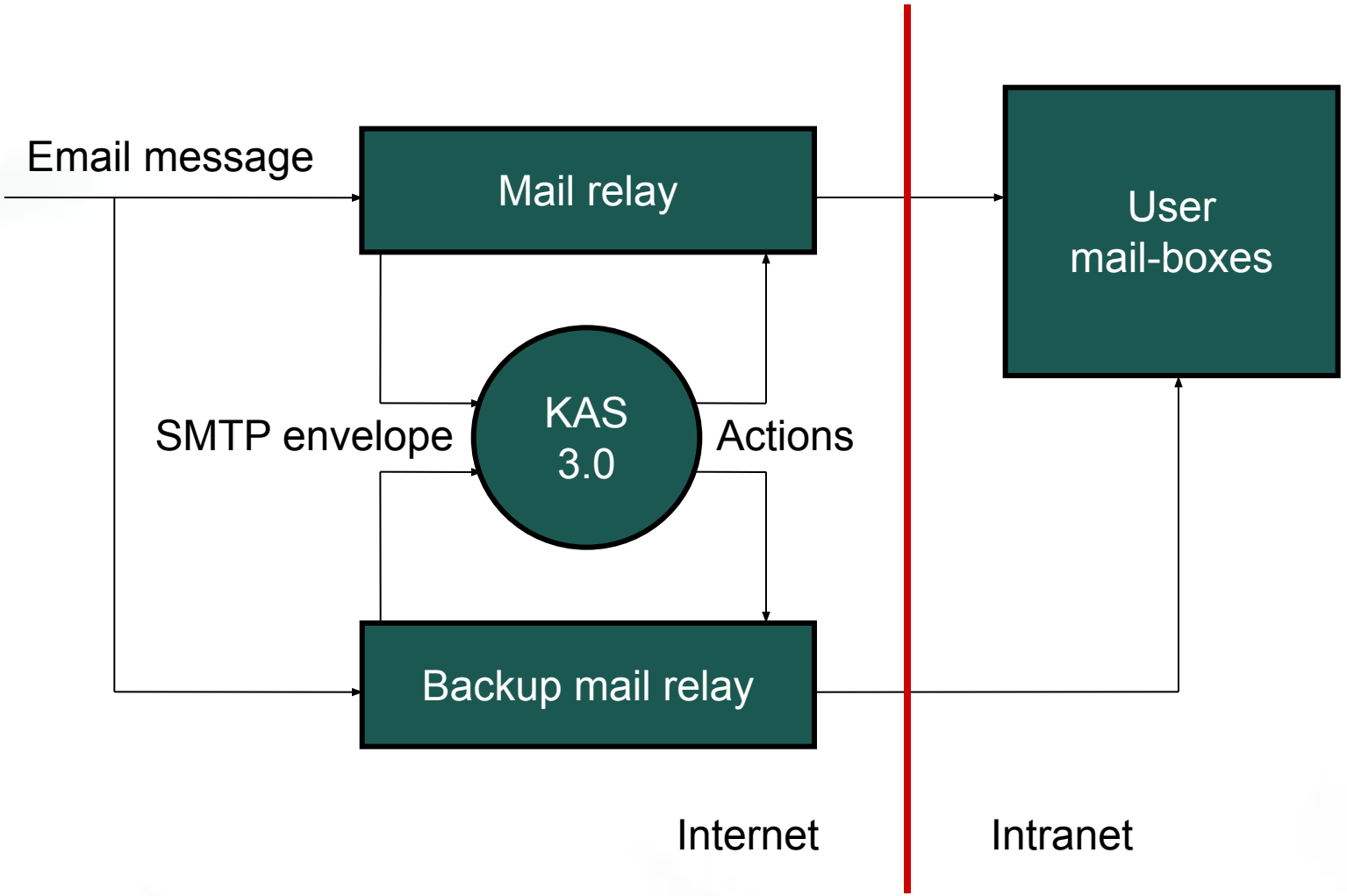
Ошибки при использовании Kaspersky Anti-Spam

- Обновления не работают или настроены реже, чем рекомендовано
- Отключена технология UDS
- Отключено использование DNSBL
- Используется устаревшая версия продукта

Глава 05
Kaspersky AntiSpam 3.0

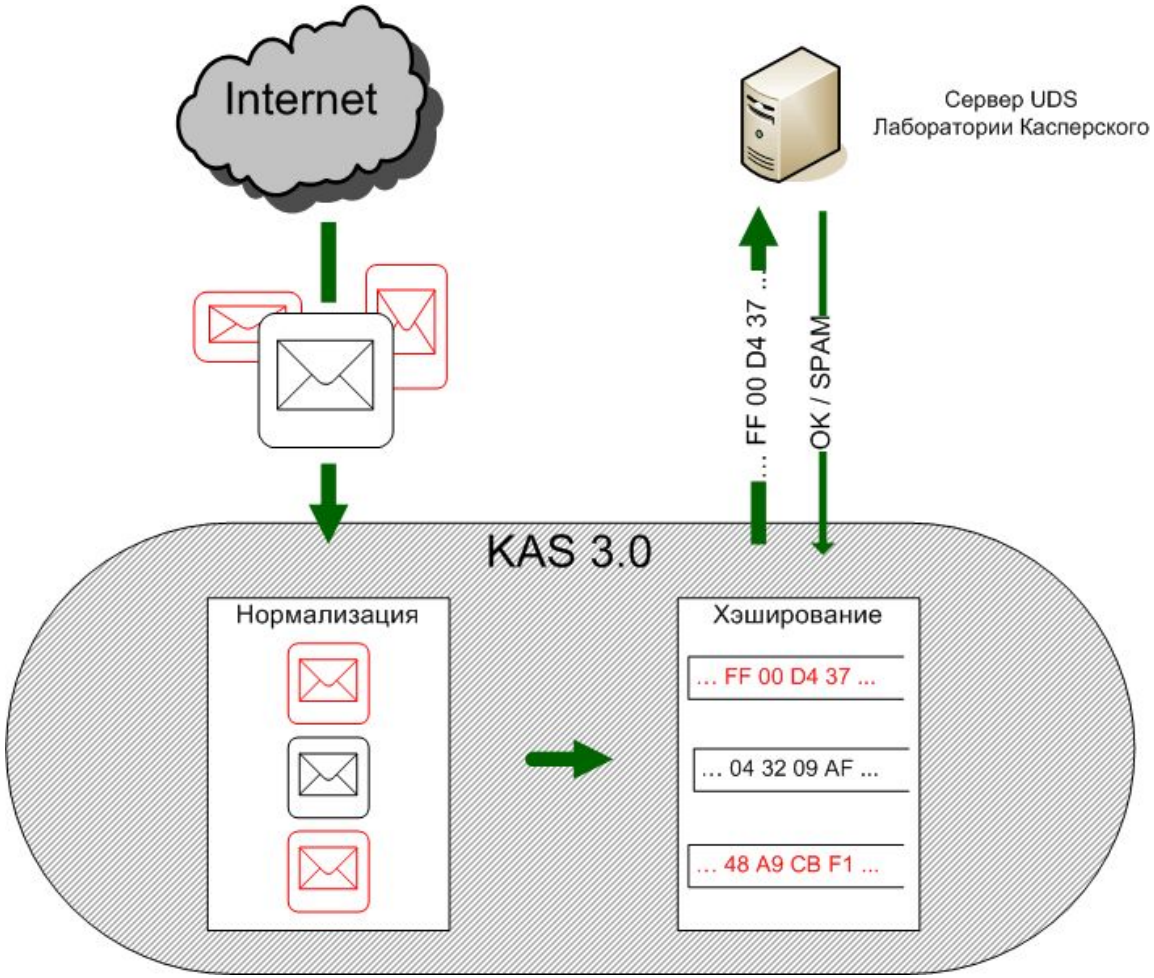
KAS в линейке продуктов Лаборатории Касперского

Схема интеграции KAS



Процесс анализа почтовых сообщений

Технология Urgent Detection System



Поддерживаемые платформы и почтовые системы

- Red Hat Linux / Fedora Core / Enterprise Advanced Server

- SuSE Linux Professional / Enterprise

- Mandrake Linux

- Debian GNU/Linux

- Free BSD 4.1 / 5.4
  6.x (using compat.x)

- Почтовые системы (MTA)
  - Sendmail
  - Postfix
  - Exim
  - Qmail
  - Communigate Pro

Системные требования

- Минимальные требования
  - Intel Pentium III 500МГц, 512Мб
- Рекомендуемая конфигурация
  - Intel Pentium IV 2.4ГГц, 1024Мб

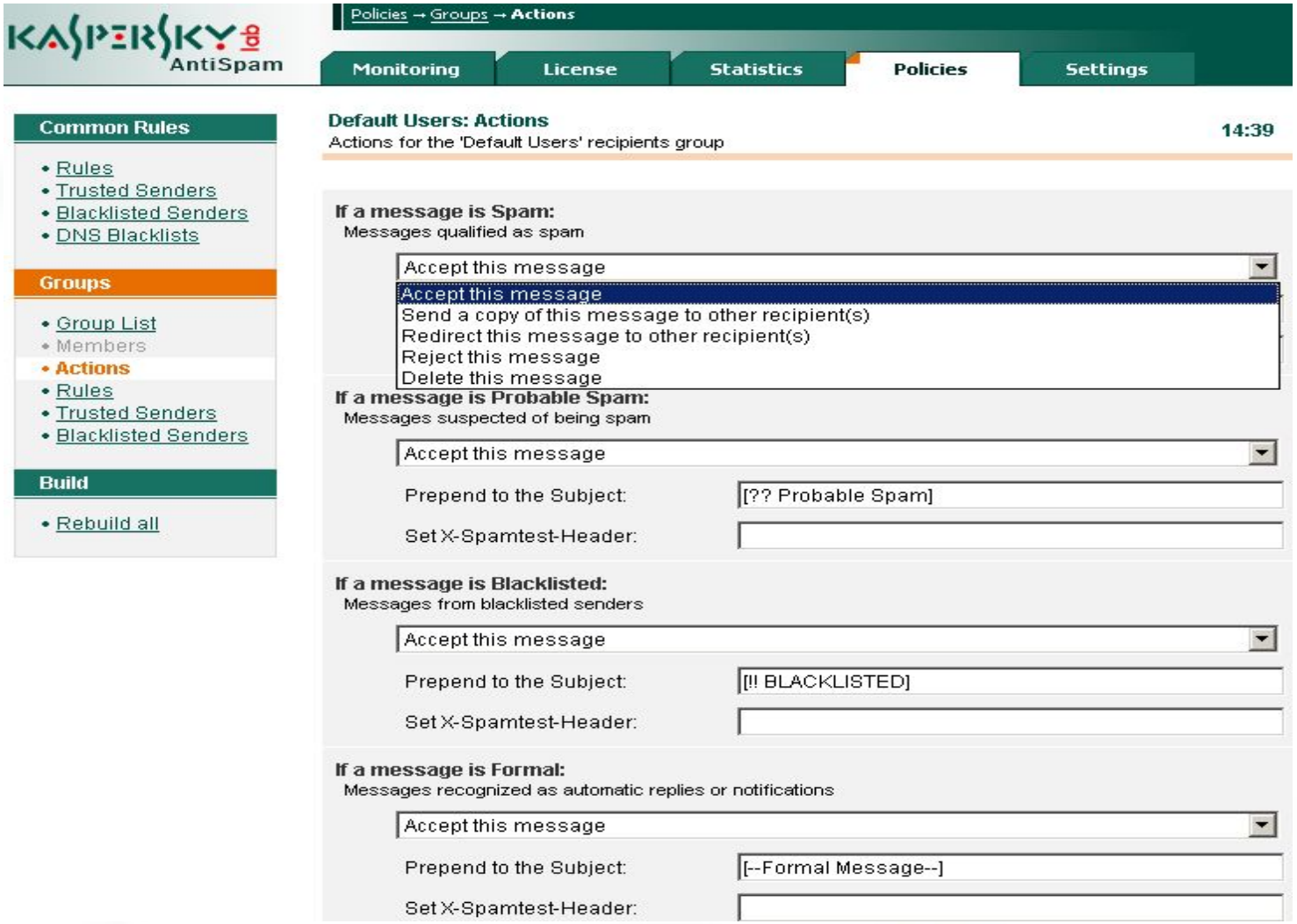
Производительность и статистика

- Производительность
  - более 2,5 млн. сообщений в сутки (сервер P4-2,6 ГГц / 512 Мб)
  - более 70 млн. сообщений в сутки (500 Гб трафика) на Mail.Ru
- Уровень обнаружения спама
  - до 97% (Checkmark Anti-Spam Premium)
- Уровень ложных срабатываний
  - менее 1 на 10 000 писем
- Размер обновлений
  - в 3,5 раза меньше, чем в версии 2.0
  - около 600 Мб в месяц

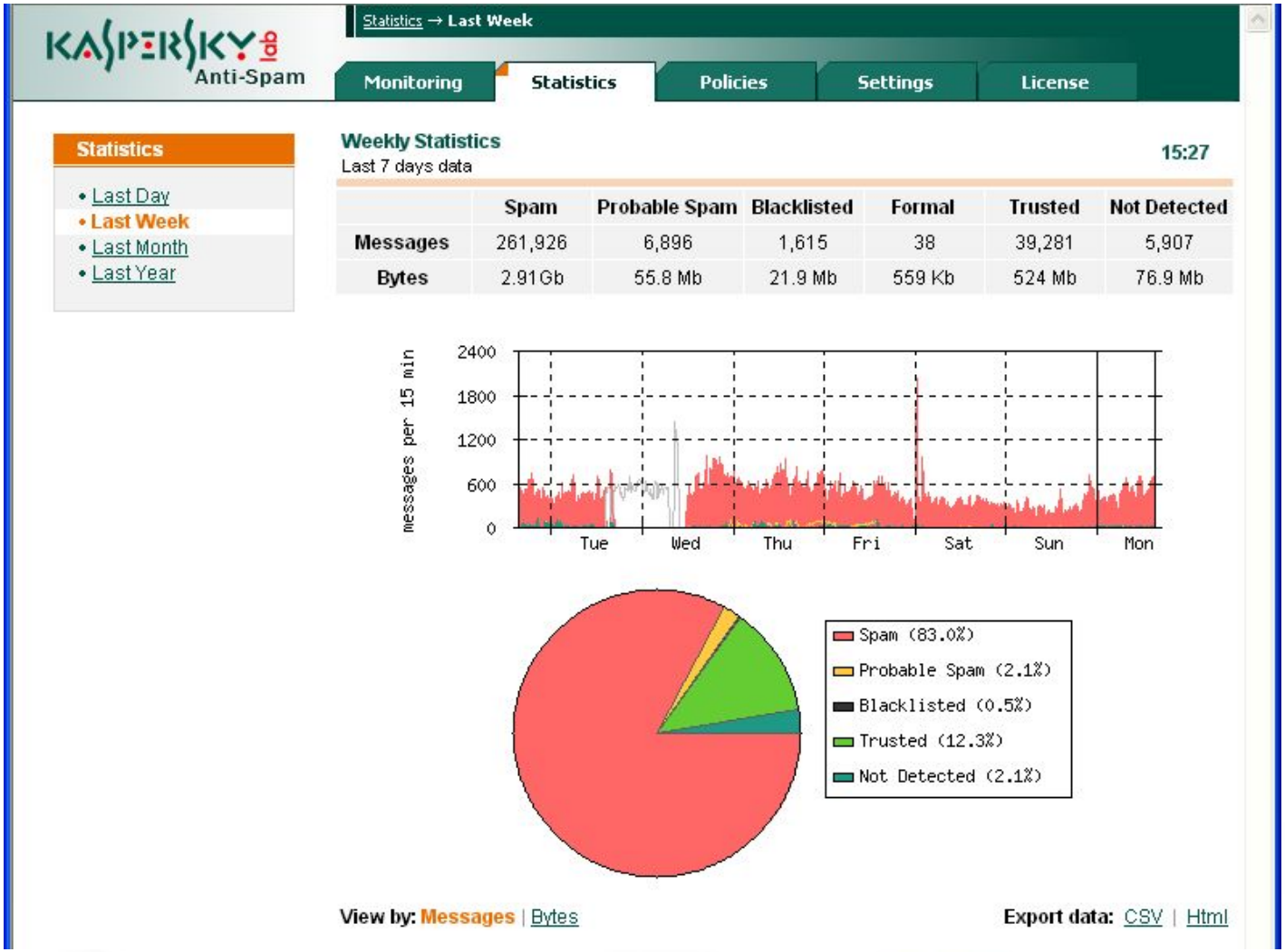
Основные возможности KAS: функционал

- Управление настройками фильтрации на основе групповых политик
- Обработка сообщений на основе присвоенного им статуса
- Веб-интерфейс
- Модуль статистики фильтрации

Веб-интерфейс



Статистика фильтрации



Спасибо!
Вопросы?
Ваше мнение.