Защита электронной почты, контроль информационного наполнения Web трафика

Центр информационных технологий
Белгосуниверситет
Крутых Александра Николаевна
тел. 209-50-98
E-mail: krutykh@bsu.by

Проблемы, связанные с использованием Интернет ресурсов

- **Источник распространения вредоносного код, почтовые черви**
- **Канал, через который осуществляются атаки**
- **Средство скрытого проникновения в корпоративные сети**
- **Канал утечки конфиденциальной информации**
- **Снижение производительности труда в коллективе**

Проблемы, связанные с использованием Интернет ресурсов

- **Источник распространения вредоносного код, почтовые черви**
  - черви для интернет-пейджеров (IM-черви, Instant Messaging)
  - черви для файлово-обменных сетей (P2P-черви, peer-to-peer)
  - троянские программы (сокрытие по stealth-технологии, например, rootkit-технологии)
  - потенциально опасные программы (riskware, greyware), например, программы дозвона (dialers), FTP-сервера, telnet-сервера, утилиты удаленного администрирования и т.п.
  - программы шпионы (spyware)
  - рекламные коды (adware)

Проблемы, связанные с использованием Интернет ресурсов

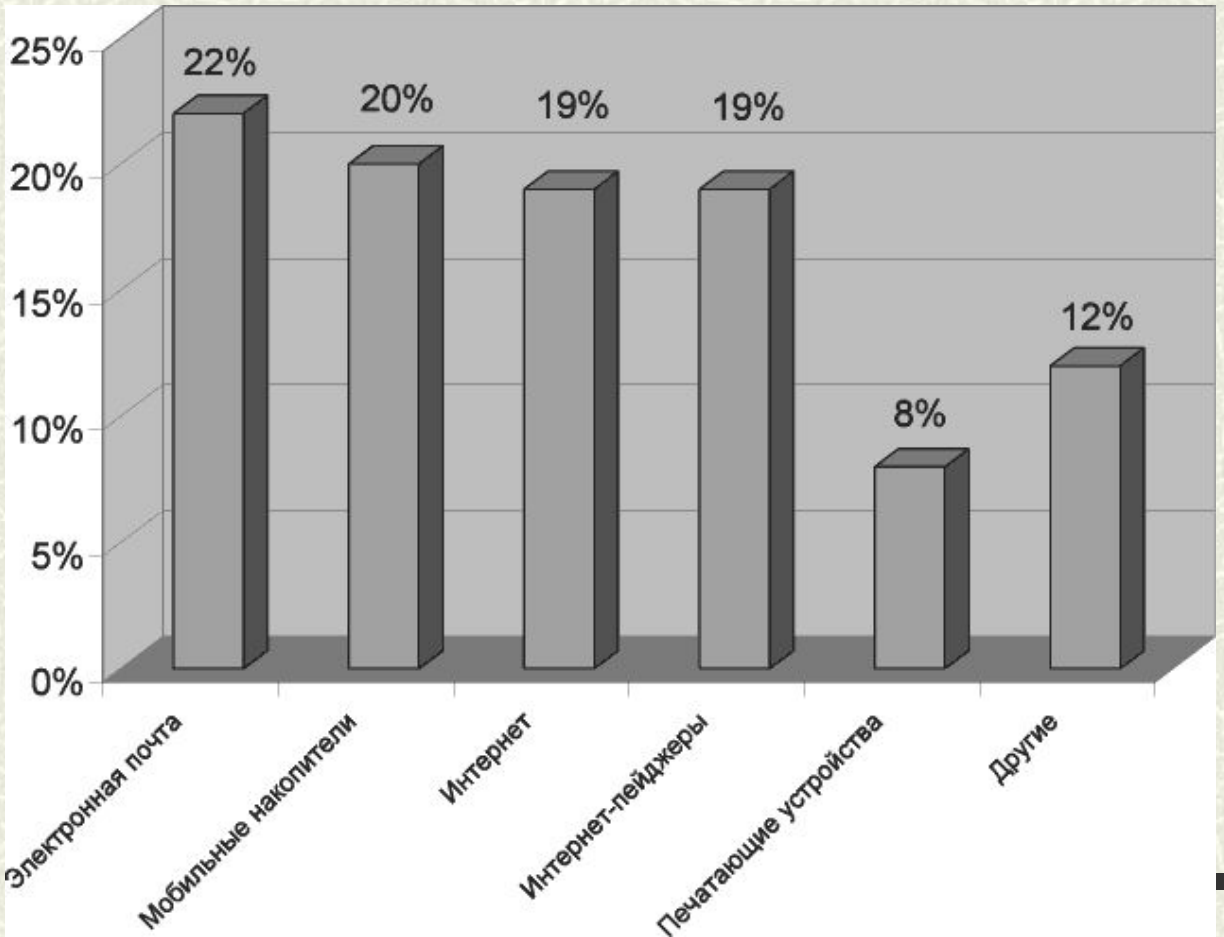
- **Канал, через который осуществляются атаки**
  - атаки с использованием социальной инженерии, т.е. человеческого фактора
  - DoS
  - фишинг – мошенничество, целью которого является получение идентификационных данных пользователей
  - вымогательство денег (Gpcode, Krotten, Cryzip.a)

Проблемы, связанные с использованием Интернет ресурсов

- **Средство скрытого проникновения в корпоративные сети**
  - spam
  - интернет-пейджеры (IM, Instant messaging)
    - AOL (AOL IM – AIM, Trillian, SameTime Connect)
    - ICQ (ICQPro, ICQ Lite)
    - Microsoft (MSN Messenger, Windows Messenger, Trillian)
    - Yahoo! (Yahoo! Messenger, Trillian)
  - распределенные сети P2P (Peer-to-peer)
    - Файловые обменные сети
    - Распределенные вычислительные сети
    - Службы сообщений
    - Сети групповой работы

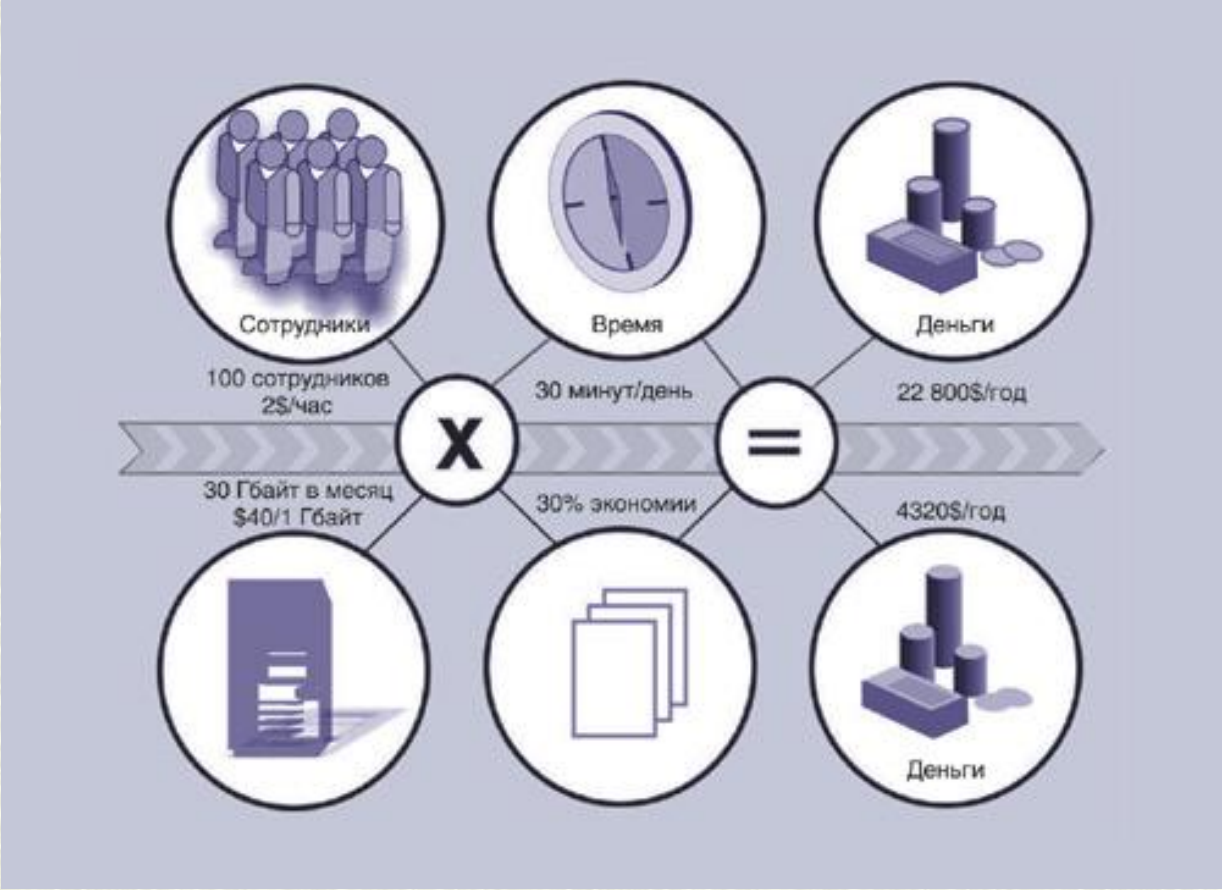
Проблемы, связанные с использованием Интернет ресурсов

- **Канал утечки конфиденциальной информации**



Проблемы, связанные с использованием Интернет ресурсов

- **Снижение производительности труда в коллективе**



Основные Интернет сервисы

- Электронная почта
- Web ресурсы
- Интернет пейджеры
- Пиринговые сети (P2P)

Системы контроля контента электронной почты

Основные функции систем контроля контента электронной почты

- **Предотвращение утечек конфиденциальной информации**
- **Защита от атак с использованием социальной инженерии (фишинг/фарминг)**
- **Защита от спама**
- **Защита от вирусов и другого вредоносного кода**

Электронная почта. Предотвращение утечек конфиденциальной информации

Методы:

- анализ текста по содержанию (т.е. по определенным ключевым словам или фразам);
- анализ формальных признаков документа (например, отправитель, получатель и т.д)
- fingerprints (цифровые отпечатки)- создание базы конфиденциальных документов-образцов, анализируемые документы проверяются на совпадение с образцами из базы

Электронная почта. Защита от атак типа фишинг/фарминг

Фишинг (*phishing)*- вид интернет мошенничества, при котором осуществляется получение личной информации от пользователей Интернета путем рассылки электронных писем, направляющих пользователей на сфальсифицированный веб-сайт.

Фарминг *(pharming)* сводится к автоматическому перенаправлению пользователей на фальшивые сайты с целью хищения конфиденциальной информации. В отличие от фишинга, фарминг-атаки практически не требуют выполнения каких-либо действий потенциальной жертвой.

Source	Percent
United States	39.9%
Australia	27.1%
United Kingdom	24.3%

Symantec Intelligence Report :: JANUARY 2014

Электронная почта. Защита от атак типа фишинг/фарминг

Методы борьбы:

- Относитесь с опаской к сообщениям, в которых вас просят указать ваши личные данные. Вероятность того, что ваш банк может запросить подобные данные по электронной почте, чрезвычайно мала. Если вы получили электронное письмо, якобы отправленное банком, перезвоните в банк и уточните, действительно ли вам посылали сообщение.
- Не заполняйте полученные по электронной почте анкеты, предполагающие ввод личных данных. Подобную информацию безопасно вводить только на защищенных сайтах. Убедитесь, что его адрес начинается с "https://"
- Не проходите по ссылкам в электронных письмах в формате HTML: киберпреступники могут спрятать адрес подложного сайта в ссылке, которая выглядит как настоящий электронный адрес банка. Вместо этого скопируйте ссылку в адресную строку браузера.
- Убедитесь, что ваше антивирусное решение способно блокировать переход на фишинговые сайты или установите интернет-обозреватель, оснащенный фишинг-фильтром.
- Регулярно проверяйте состояние своих банковских счетов (в том числе счетов, к которым привязаны дебетовые и кредитные карты) и просматривайте банковские выписки, чтобы убедиться в отсутствии "лишних" операций.
- Связывайтесь с банком по телефону всякий раз, когда ситуация покажется вам подозрительной.
- Следите за тем, чтобы у вас всегда была установлена последняя версия интернет-обозревателя и все обновления безопасности.

Электронная почта. Защита от спама

Признаки определения спама:

- сообщение является массовой рассылкой;
- сообщение рассылается без согласия пользователя;
- сообщение содержит рекламу;
- сообщение является анонимным.

Электронная почта. Что не попадает под спам

- Рассылки, на которые пользователь когда-то подписывался (даже если он уже не хочет ее получать и/или забыл, как отписаться).
- Технические сообщения систем электронной почты, включая сообщения о недоставке писем, которые пользователь не рассылал (во время последних вирусных эпидемий такие случаи участились).
- Технические сообщения антивирусных систем о том, что в письме найден вирус.
- Уведомления о доставке, недоставке или прочтении писем получателем.

Доля спама в почтовом трафике

Январь 2014 в цифрах (от Symantec Corporation)

Доля спама в почтовом трафике в январе 2014 составила 62,1 (февраль 2013 - 71,1%).

Geography	Percent
Sri Lanka	74.7%
Israel	68.8%
Brazil	66.9%
South Africa	65.3%
Kuwait	64.8%

Доля спама в почтовом трафике

Январь 2014 в цифрах (от Symantec Corporation)

По категориям:

Категория	Процент
Порно/Знакомства	75.2%
Реклама фармацевтических препаратов	20.1%
Работа	1.8%

По доменам:

Месяц	.com	.info	.ru	.biz
Декабрь	33.1%	13.7%	13.2%	10.3%
Ноябрь	36.7%	12.4%	нет	9.6%

Электронная почта. Чем вреден спам

- Паразитный трафик. 60-70% входящих сообщений - спам.
- Снижение производительности компании.
- Случайная потеря важных сообщений при ручной чистке электронной почты.
- Угроза стабильности работы почтовых серверов.
- Опасное содержание: вирусы, трояны, запрещенные материалы.

Электронная почта. Многофакторный анализ

- Уровень заголовка
- Уровень тела письма
- Вложение

Методы защиты от спама

Проверка отправителя:

- Определение Зомби сетей (botnets)
- Механизм IP репутации
- Методы аутентификации почтовых серверов
- Механизм DNSBL (DNS blacklist)
- Механизм “белых” и “черных” списков

Анализ сообщения:

- Детектирование массовых рассылок
- Лингвистические методы
- Механизм SURBL (Spam URI Realtime Blocklists)

Защита от спама. Проверка отправителя

Технологии аутентификации почтовых серверов с использованием DNS

- аутентификация по IP адресу сервера отправителя:
  - Sender Policy Framework (SPF)
  - SenderID
- криптографическая аутентификация отправителя:
  - DomainKeys Identified Mail (DKIM)

Защита от спама. Проверка отправителя

Метод SPF (RFC4408)

1. Администратор (владелец) домена публикует данные, описывающие возможные источники электронной почты с адресами отправителя из этого домена.
2. Почтовый сервер, принимающий E-mail с адресом отправителя из данного домена, может сопоставить реальный источник сообщения (IP-адрес стороны, посылающей почту) с данными, которые опубликовал владелец домена.
3. Результатом анализа SPF-политики на принимающей стороне является SPF-статус сообщения, который может иметь одно из следующих значений:

   Pass - отправитель сообщения не подделан (согласно анализу SPF-политики).

   Softfail - сообщение не отвечает "жестким" критериям достоверности отправителя, но нельзя и быть уверенным, что отправитель подделан.

   Fail - отправитель подделан.

Защита от спама. Проверка отправителя

Метод SPF. Запись в DNS.

domain.name. IN TXT "v=spf1 ip4:192.168.0.2/32 +a:www.another.domain.com -all"

Данный пример означает:

1. Поддержан протокол SPF версии 1 (v=spf1);
2. Почта с From: someuser@domain.name может приходить (рекомендовано принимать) с:

a. IP-адреса 192.168.0.2/32

b. Сервера с именем www.another.domain.com

Не рекомендовано принимать более ниоткуда (**-all**).

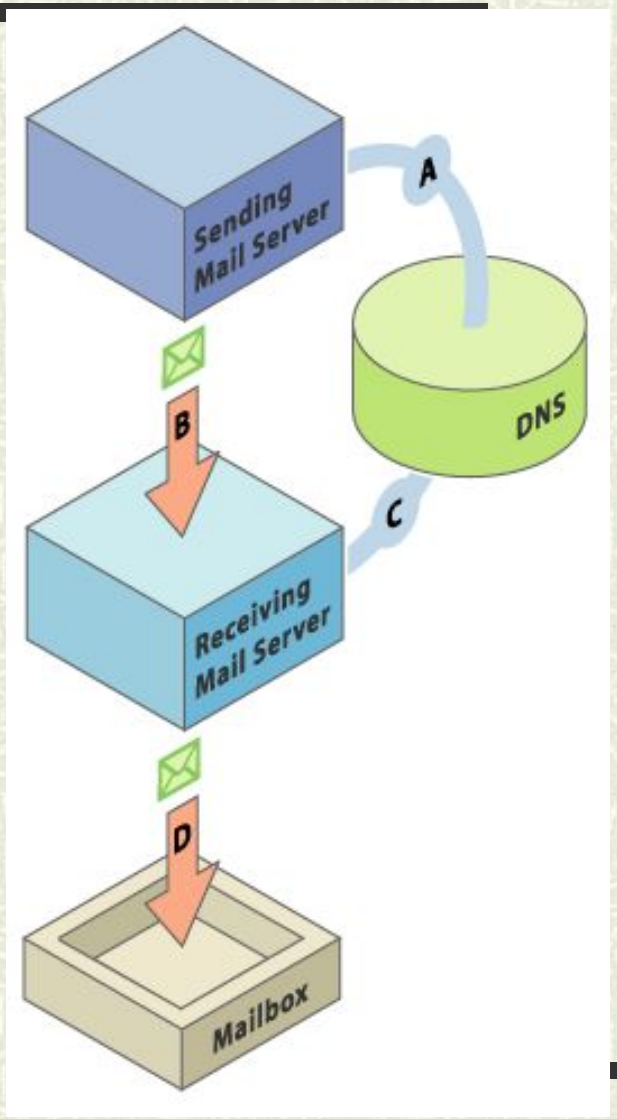
Защита от спама. Проверка отправителя

Проверяет “from”, содержащиеся в теле сообщения e-mail, а не только адреса отправителя уровня SMTP (envelope sender).

Защита от спама. Проверка отправителя

Метод DomainKeys Identified Mail (DKIM) RFC4870, RFC4871

1. Владелец почтового сервиса (отправитель) генерирует пару криптоключей (публичный и приватный).
2. Публичный ключ публикуется в DNS, а приватный ключ используется на почтовых серверах для пометки всей исходящей корреспонденции. К заголовку каждого письма добавляется DKIM-Signature, которая есть электронная подпись заголовка и тела письма.
3. Другая сторона (получатель) извлекает из поля «From» имя домена и отправляет запрос к серверу DNS, чтобы получить публичный ключ для этого домена, после чего проверяет подлинность подписи в заголовке почтового сообщения.



Защита от спама. Проверка отправителя

Пример записи в DNS:

```
beta._domainkey.gmail.com IN txt
"t=y; k=rsa;
p=MIGfMA0GCSqGSIb3DQEBAQUAA4…”
```

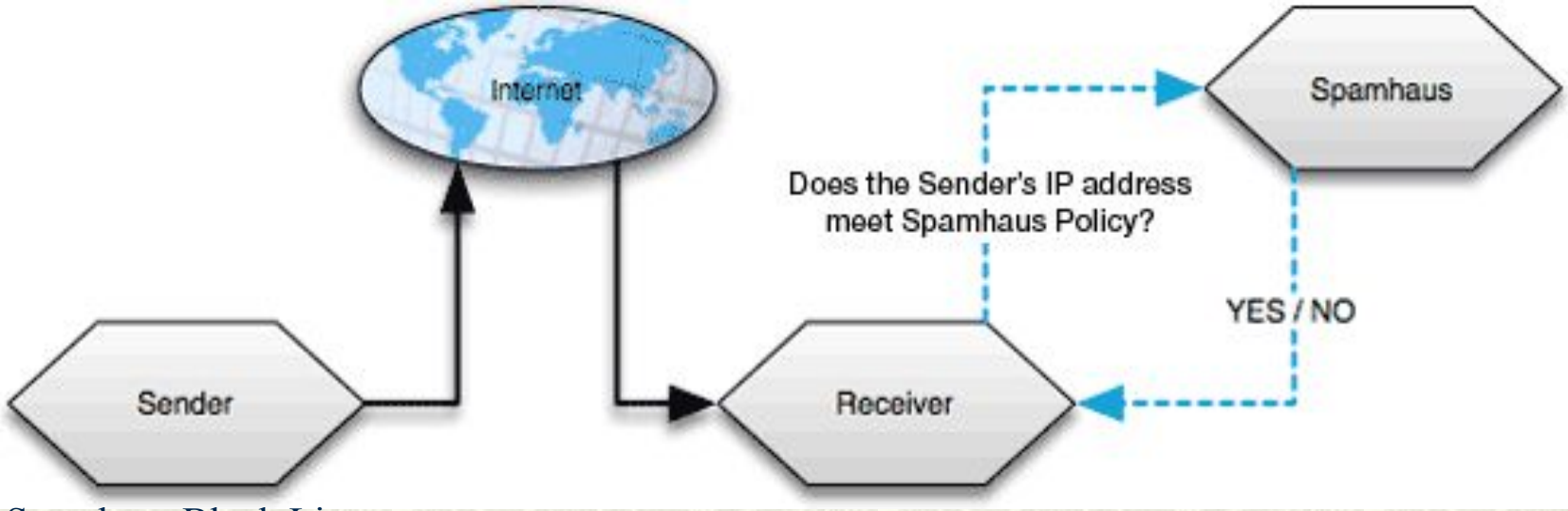
Заголовок почтового сообщения DKIM:

```
DomainKey-Signature: a=rsa-sha1;
c=nofws;  s=beta; d=gmail.com;
h=received:message-id:date:from...
b=Gjon4OA2c8NfLCBauZskv99Eks....
```

Защита от спама. Проверка отправителя

Фильтрация почты по распределенным черным спискам DNSBL

http://www.spamhaus.org
http://www.spamcop.net
http://cbl.abuseat.org
http://dnsbl.sorbs.net



SBL Spamhaus Block List – спам машины и подсети
XBL Exploits Block List – инфицированные машины, открытые прокси различных видов
PBL Policy Block List – диапазоны IP адресов, с которых не рекомендуется принимать почту

Защита от спама. Проверка отправителя

Фильтрация почты по распределенным черным спискам DNSBL

```
C:\Documents and Settings\krutix>nslookup
Default Server:  bsuad.bsu
Address:  10.0.0.20
> mail.bsu.by
Server:  bsuad.bsu
Address:  10.0.0.20
Non-authoritative answer:
Name:    mail.bsu.by
Address:  217.21.43.4
> 4.43.21.217.spamhaus.org
Server:  bsuad.bsu
Address:  10.0.0.20

Non-authoritative answer:
Name:    blocklist.address.is.wrong.spamhaus.org
Address:  127.0.0.2
Aliases:  4.43.21.217.spamhaus.org
```

Защита от спама. Проверка отправителя

Метод GreyListing

- Почтовый сервер отклоняет сообщение в момент прибытия с ошибкой 4xx
- Помещает в базу GreyListing следующие данные:
  - IP-адрес сервера, отправляющего почту
  - почтовый адрес отправителя
  - почтовый адрес получателя
- Легитимный сервер, отправляющий почту повторяет попытку посылки сообщения, т.к. получил ошибку 4xx
- Сервер получатель по базе GreyListing проверяет вновь полученное сообщение, авторизация прошла – почта доставляется получателю

Защита от спама. Анализ сообщения

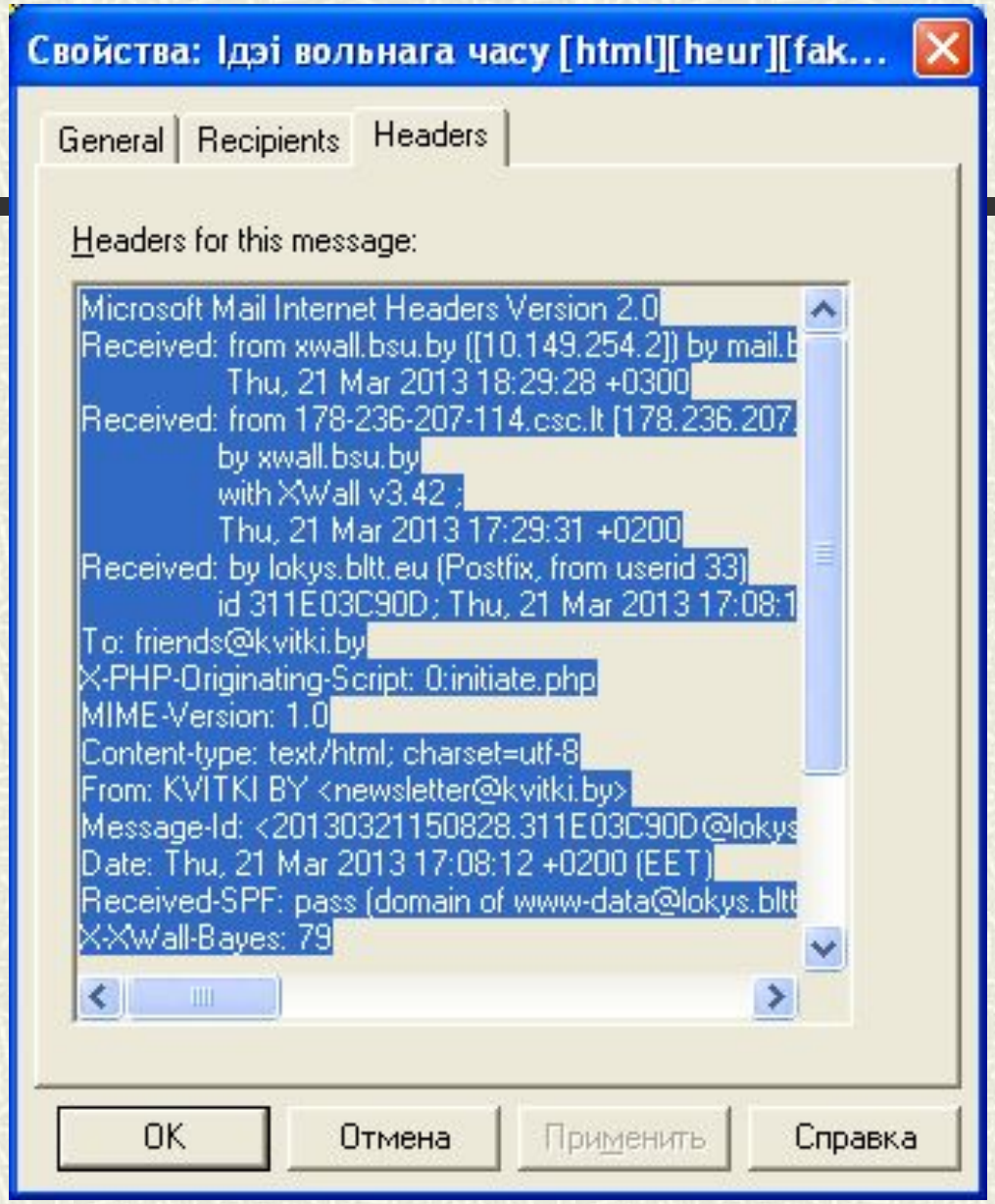
Детектирование массовых рассылок

Задачей детекторов массовой рассылки является обнаружение рассылки похожего письма большому количеству абонентов.

- Distributed Checksum Clearing house (DCC) http://www.rhyolite.com/anti-spam/dcc

Для каждого входящего сообщения определяется контрольная сумма и отправляется на DCC-сервер, при сравнении контрольной суммы сервер определяет, сколько раз подобное письмо уже приходило в систему, и по достижении определенного порога прием подобных писем блокируется.

- Razon

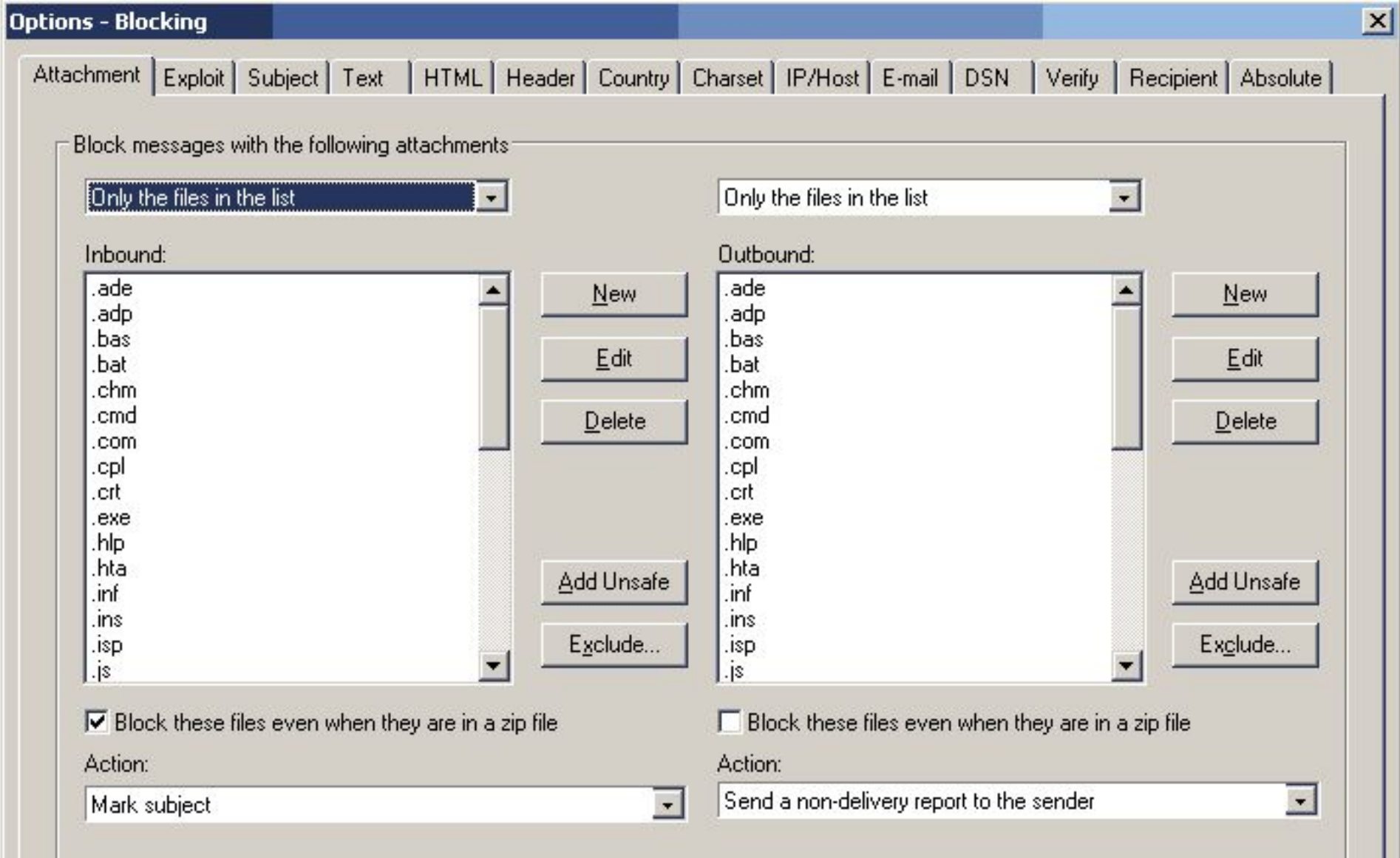

Свойства: Ідэі вольнага часу [html][heur][fak...
General
Recipients
Headers
Headers for this message:
Microsoft Mail Internet Headers Version 2.0
Received: from xwall.bsu.by ([10.149.254.2]) by mail.b
Thu, 21 Mar 2013 18:29:28 +0300
Received: from 178-236-207-114.csc.lt [178.236.207.
by xwall.bsu.by
with XWall v3.42 ;
Thu, 21 Mar 2013 17:29:31 +0200
Received: by lokys.bltt.eu (Postfix, from userid 33)
id 311E03C90D; Thu, 21 Mar 2013 17:08:1
To: friends@kvitki.by
X-PHP-Originating-Script: 0:initiate.php
MIME-Version: 1.0
Content-type: text/html; charset=utf-8
From: KVITKI BY <newsletter@kvitki.by>
Message-Id: <20130321150828.311E03C90D@lokys
Date: Thu, 21 Mar 2013 17:08:12 +0200 (EET)
Received-SPF: pass (domain of www-data@lokys.bltt
X-XWall-Bayes: 79
OK
Отмена
Применить
Справка

Защита от спама. Анализ сообщения

Формальные методы защиты от спама

- Отсутствие адреса отправителя
- Отсутствие или слишком большое число получателей
- Отсутствие IP адреса в системе DNS
- Фальшивые или некорректные заголовки
- Фильтрация по размеру сообщения
- Фильтрация по формату сообщения

Формальные методы защиты от спама. Фильтрация по формату сообщения

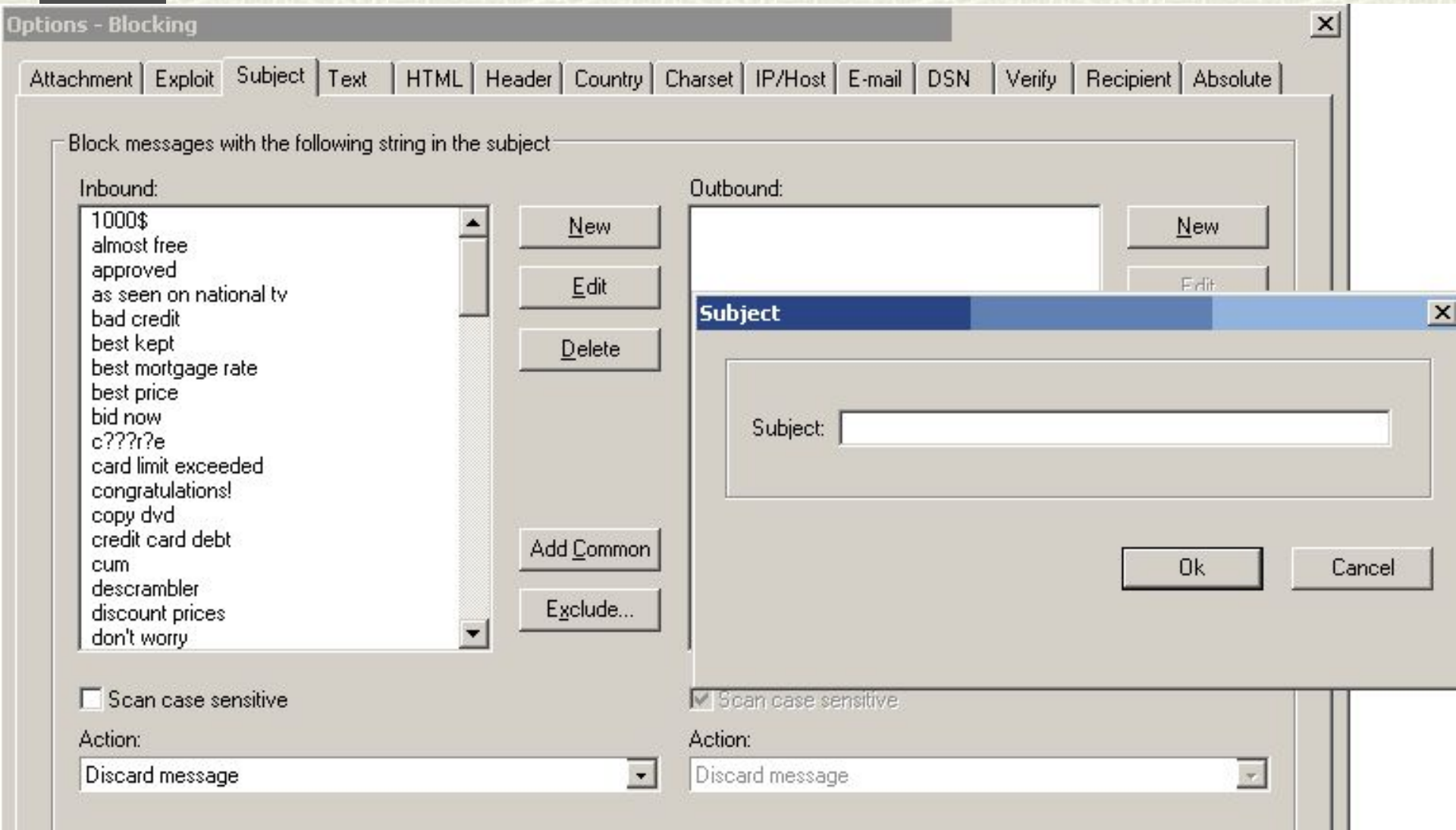


Защита от спама. Анализ сообщения

Лингвистические методы

- Фильтрация на основе сигнатур
- Контентная фильтрация

Защита от спама. Анализ сообщения



Защита от спама. Анализ сообщения

Контентная фильтрация:

- Статистический метод (Statistical Token Analysis – STA)
- Метод Байеса (Bayes).

Теорема Байеса — одна из основных теорем элементарной теории вероятностей, которая определяет вероятность наступления события в условиях, когда на основе наблюдений известна лишь некоторая частичная информация о событиях.

$Z = A/(A+B)$,

где $A = z1*z2*...*zn$,

$B = (1-z1)*(1-z2)*...(1-zn)$,

zn - спам-оценка каждого слова, входящего в письмо.

Защита от спама. Анализ сообщения

Фильтрация по спискам URL доменов SURBL (spam URL real-time blacklists)

http://www.surbl.org


Все сообщения
Spam
Черные списки.
Распознование
30-40%
Много ложных
тревог
Формальные
признаки.
Распознавание
30-40%
Средний
уровень ложных
тревог
Сигнатуры.
Распознава-
ние 15-20%
нет ложных
тревог
Контентный
анализ.
Разпознование
50-70%
Малое количество
ложных тревог

Простые правила защиты от спама

1) Заведите почтовый адрес не на бесплатном сервисе.
2) Никогда и ни под каким видом не публикуйте этот адрес на www-страничках (не указывайте его в письмах на форумах, не ставьте его на своих страничках, не ставьте его в подписи письма). Если же вам позарез нужно опубликовать адрес в ответ на какое-то письмо в форуме - публикуйте его через пробелы: имя @ домен.ru - в этом случае он не попадет в спамерскую базу.
3) Никогда не указывайте этот адрес в формах регистрации на различных серверах. Заведите отдельный бесплатный адрес - только для регистраций - и используйте именно его.

Системы контроля контента электронной почты

Функции:

- декомпозиция электронного письма
- анализ содержимого каждого компонента
- фильтрация
- реагирование
- ведение архива переписки по электронной почте.

Защита электронной почты– организационные меры в сочетании с техническими средствами

Для защиты компании от рисков, связанных с использованием электронной почты, необходимы:

Политика использования электронной почты **+** Средство реализации политики

СТБ П 34.101.4-2002 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты электронной почты предприятия. 01.07.2010

Системы контроля Web контента

Системы контроля Web контента

- **Борьба с утечкой конфиденциальной информации**
  - фильтрации содержимого информации, исходящей из корпоративной сети вовне;
  - блокирования доступа к любой группе ресурсов, которые считаются опасными в связи с принятой в компании политикой безопасности. К таким ресурсам относятся, например: бесплатные почтовые сервисы; файлообменные сайты; социальные сети (например: www.odnoklassniki.ru, http://moikrug.ru); live journals (ЖЖ); IM (ICQ, jabber, msn и т. д.).

Системы контроля Web контента

- **Обеспечение безопасности использования Интернет-ресурсов**
  - блокировка Интернет-ресурсов, содержание которых нежелательно или подозрительно;
  - фильтрация информации, передаваемой по каналу HTTP, по адресам, форматам и содержимому;
  - антивирусная проверка;
  - мониторинг активности пользователей;
  - протоколирование действий пользователей;
  - оповещение о нарушении политики безопасности.

Системы контроля Web контента

- **Повышение производительности и экономия средств**
  - категоризация и блокирование доступа к сайтам, не связанным с работой;
  - блокирование загрузки файлов, не относящихся к работе;
  - установка ограничений на типы скачиваемых файлов и на объем пользовательского трафика;
  - получение реальной картины использования сотрудниками Интернет-ресурсов.

Системы контроля Web контента

Основные функции:

- Классификация трафика, приходящего из Интернет
  - Проверка IP, протоколов, URL, типов и объема данных
  - Анализ содержания текстов
  - Распознавание графики
  - Антивирусная проверка
- Разграничение доступа для определенных категорий пользователей
- Действие системы

Алгоритм работы системы контроля Web контента

1. «Паук» crawler ползает по Сети
2. Загрузка страниц в компьютерный центр
3. Анализ содержания текстов и изображений этого сайта и их классификация
4. Создание БД по категориям сайтов
5. Обновление БД
6. Пользователь просматривает Интернет-ресурсы
7. Инициируется адаптация БД

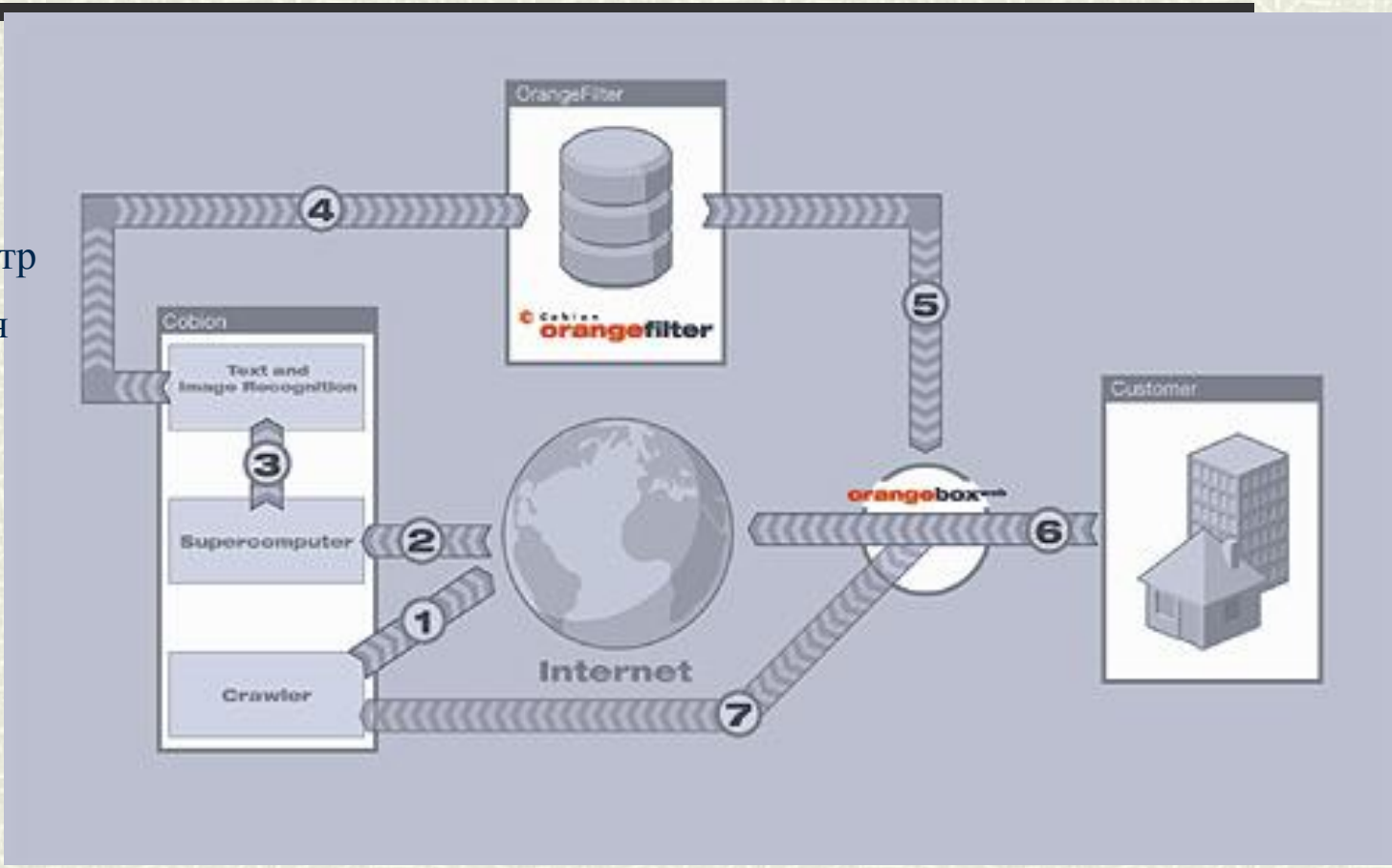
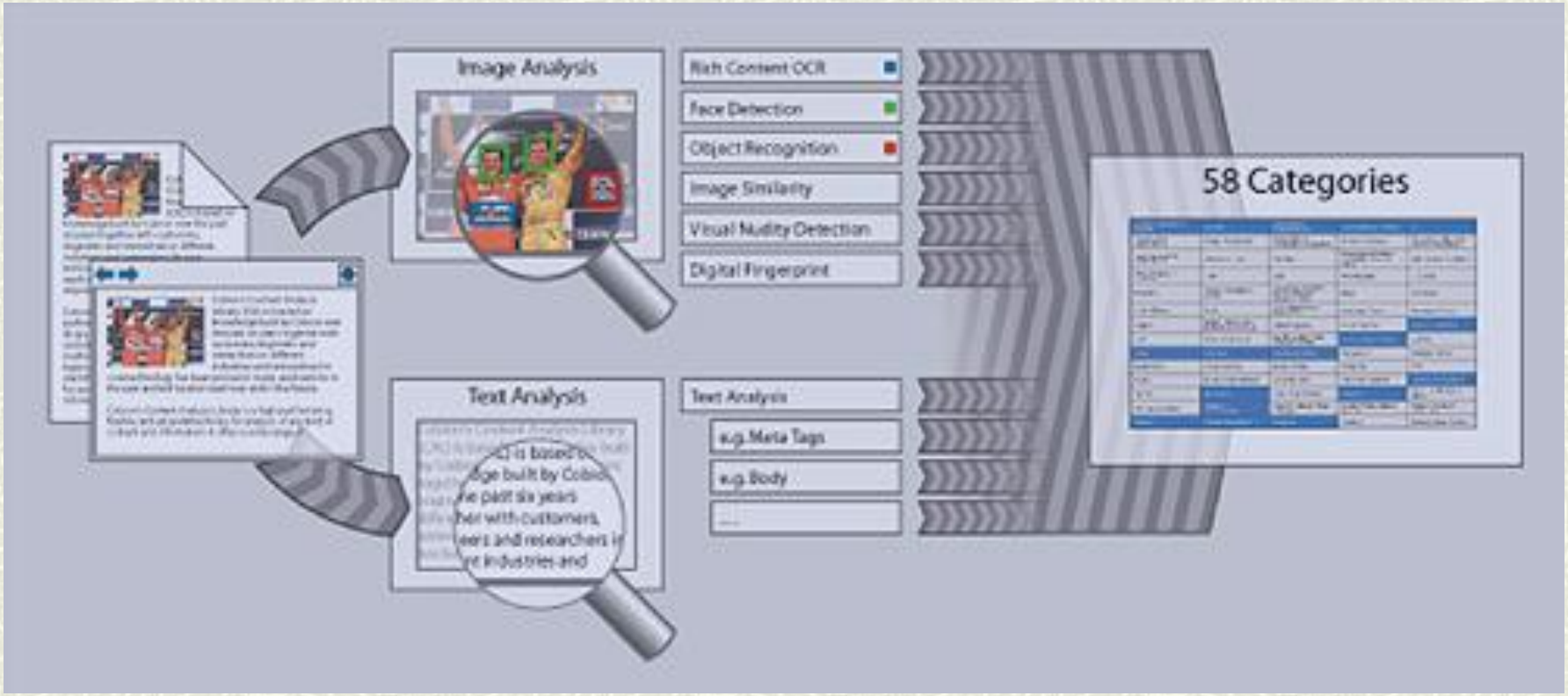


Схема классификации содержимого Интернета по категориям



Пример категорий Web контента

- Азартные игры
- Алкоголь
- Армия
- Автомобили/Транспорт
- Бизнес/услуги
- Благотворительные фонды
- Вебпочта
- Видео
- Вирусные и вредоносные сайты
- Для взрослых/эротика
- Дом/Досуг
- Загрузки
- Здоровье
- Знакомства
- Игровые порталы
- Компьютеры и Технологии
- Криминальная деятельность/хакерство
- Личные веб-страницы
- Магазины
- Музыка
- Наркотики
- Насилие
- Нецензурная речь
- Новости
- Образование и обучение
- Оружие
- Переводы
- Поиск работы
- Поисковые движки
- Политика и Закон
- Порнография/секс
- Правительство
- Путешествия
- Религия
- Риэлторские услуги
- Сайты знакомств
- Сообщества
- Социальные сети
- Спамерские сайты
- Спорт и Отдых
- Табак
- Фармация
- Финансы
- Фишинг
- Чат
- Юмор

Настройка правил

Технологии фильтрации IM и P2P трафика

- Детектирование протокола передачи данных
- Мониторинг соединений на портах, характерных для IM и P2P трафика
- Проверка сигнатур передаваемых файлов
- Антивирусная проверка
- Фильтрация на основе смыслового анализа текстов сообщений
- Блокировка спима (спам для IM)

Обзор систем контентной фильтрации

Websense	Websense, Inc
SurfControl Web Filter	SurfControl
eSafe Web Security Gateway	Aladdin
ProventiaT Web Filter	Internet Security Systems
IronPort S	Cisco (IronPort System)
InterScan Web Security Suite	TrendMicro

Проблемы с русскоязычным контентом

- неполнота базы данных русскоязычных ресурсов;

- систематическая погрешность категорирования сайтов, связанная с неучетом российских социально-политических реалий;

- систематическая погрешность категорирования сайтов, связанная, как правило, с полностью автоматическим определением категорий русскоязычных сайтов;

- низкая оперативность обновления.