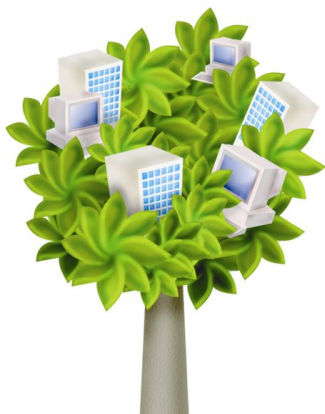
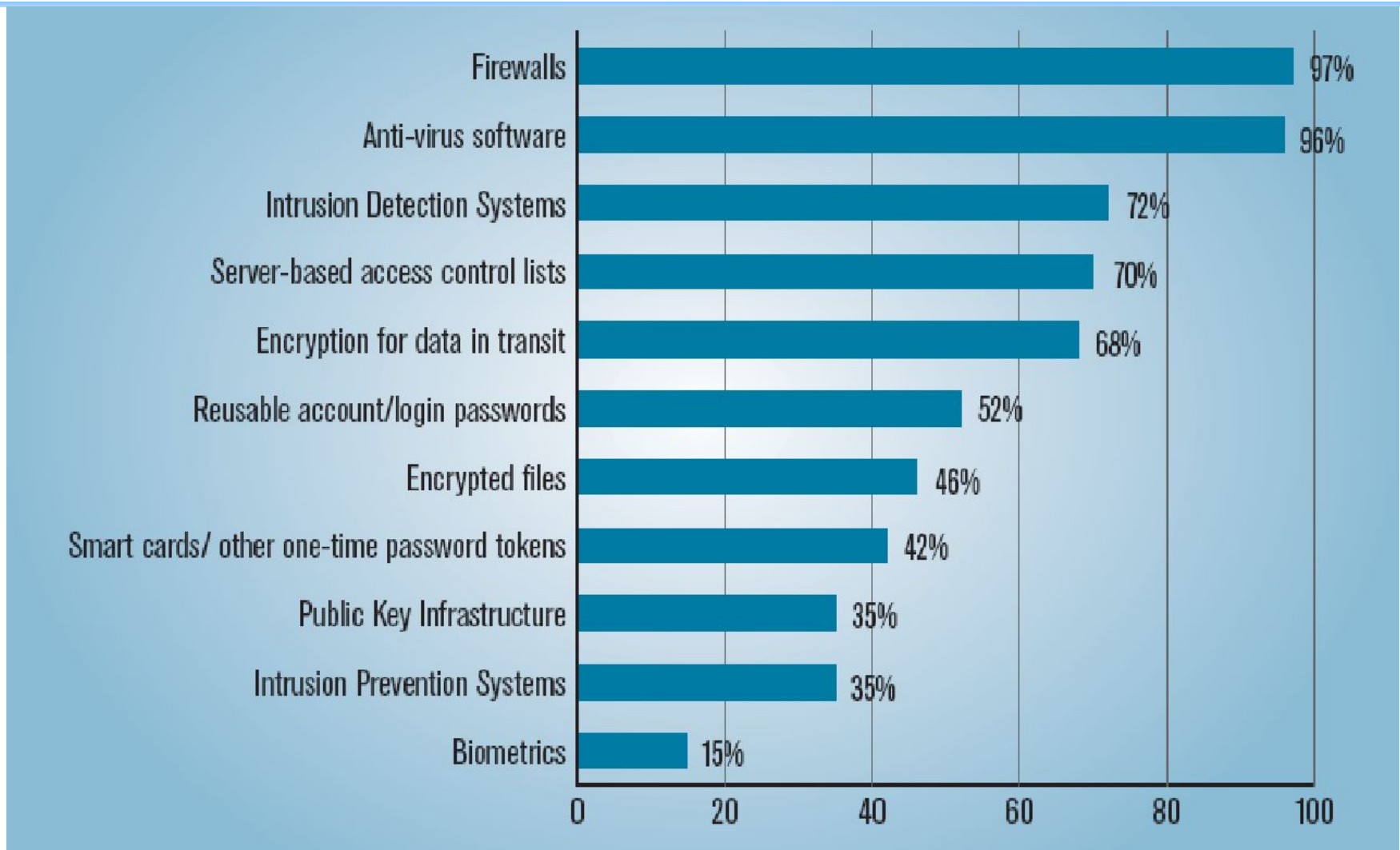


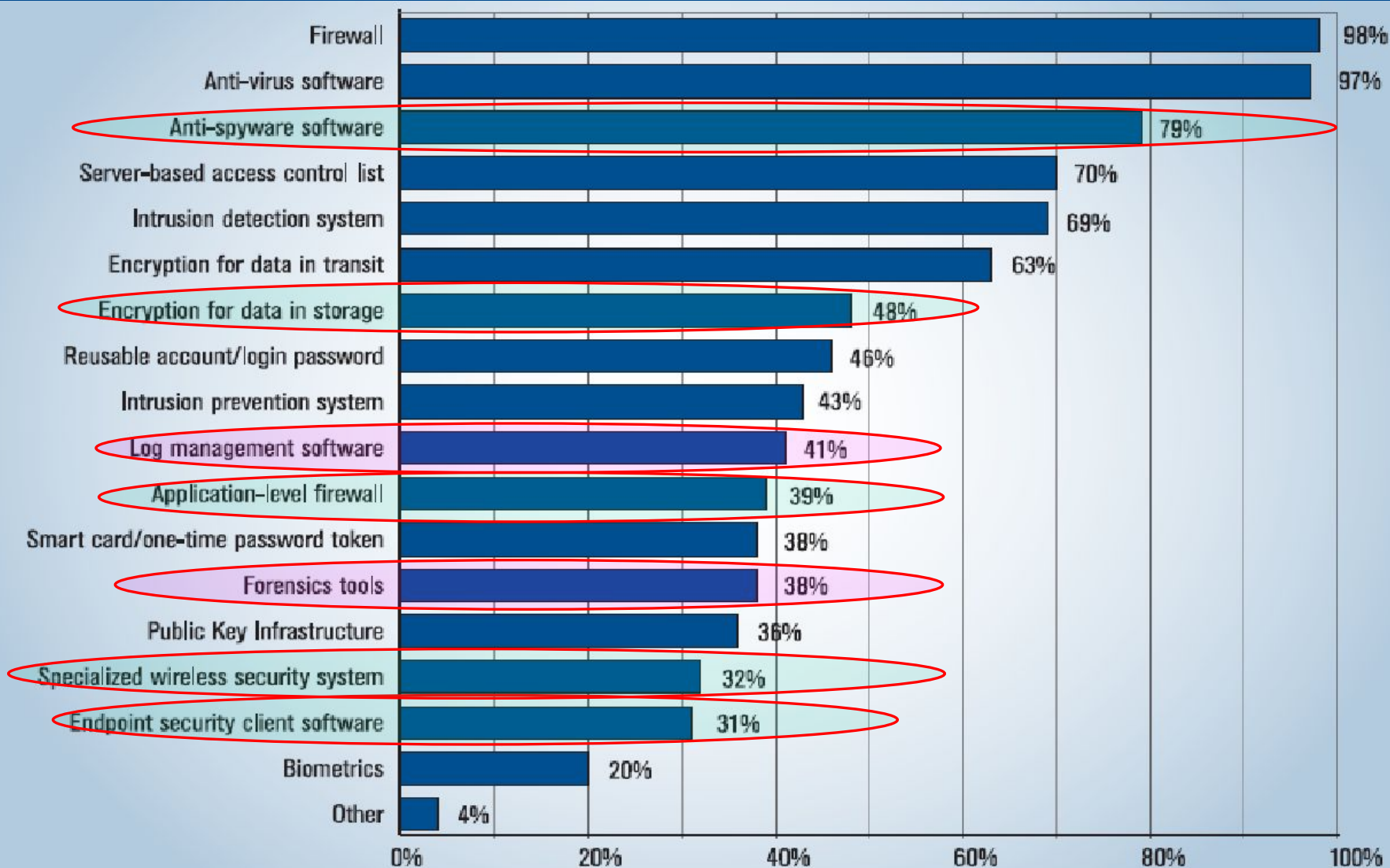


Информационная безопасность - от лоскутных подходов  
к интегрированным и комплексным решениям



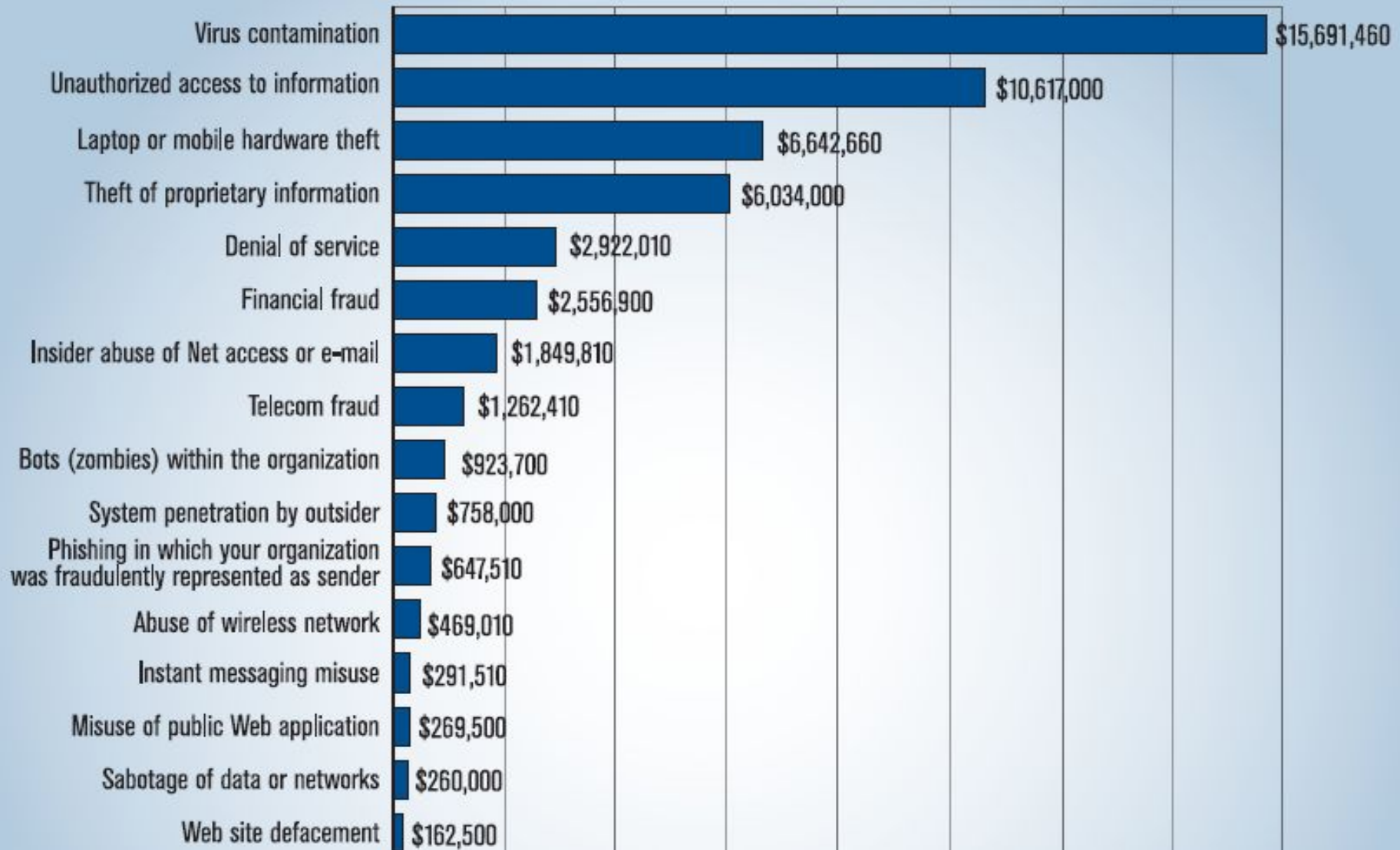


# Что используется для защиты информации в 2006 году



- **Информация становится все более важной и дорогой.** Разглашение данных, например, о клиентах или их утрата может очень дорого стоить.
- **Сети являются частью инфраструктуры,** критичной с точки зрения сбоев в работе. Нарушение работоспособности сети в течение нескольких часов может сильно ударить по доходам компании.
- **Хакерство становится все более криминальной профессией.** Все больше атак выполняются с целью получения денег.
- **Сложность систем становится врагом компании.** Чем более сложна система, тем более она уязвима к различным типам атак.
- **Появление и распространение новых атак осуществляется быстрее, чем выпуск патчей.**
- **Вредоносное ПО становится более «умным»,** чем ранее. Оно содержит анализаторы уязвимостей, которые могут быть использованы для взлома, и сканирует сети на наличие этих уязвимостей.
- **Внутренние пользователи** сетей или систем сейчас рассматриваются как **основные источники потенциальных угроз.**
- **Все большее значение начинают приобретать регламентирующие документы (ISO 27001, Sarbanes-Oxley Act и др.)** по вопросам обеспечения информационной безопасности организации.

# Потери от разных видов атак

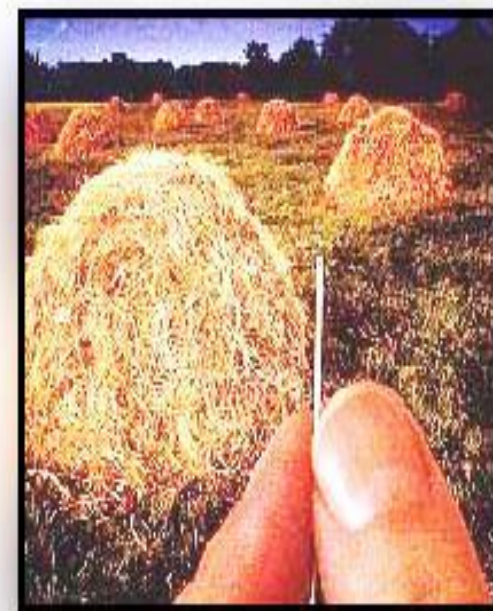


# Современная система безопасности состоит из следующих элементов:

- Подсистема межсетевого экранирования и создания **VPN**
- Подсистема обнаружения сетевых вторжений
- **Host based** система предотвращения вторжений к серверам
- Подсистема антивирусной защиты
- Подсистема аутентификации и авторизации пользователей, разграничения доступа пользователей к ресурсам ЦОД
- Подсистема централизованного мониторинга и управления событиями информационной безопасности ЦОД
- Подсистема анализа защищенности на сетевом уровне и уровне приложений
- Подсистема управления политиками безопасности (комплекс настроек сетевого и серверного оборудования с учетом требований безопасности)
- Подсистема управления обновлениями безопасности
- Подсистема защиты от СПАМА и вредоносного контента
- Подсистема контроля доступа к сайтам, блокирование **spyware**, вирусов, фишинга и вирусных атак (защита от утечек)
- Подсистема контроля систем мгновенного обмена сообщениями (**IM**)
- Система контроля утечек корпоративной информации
- Система управления учетными записями (**Identity management**)
- Система резервного копирования и восстановления

- огромные объемы данных
- растущее количество ложных срабатываний
- огромное количество сохраненных данных

Все это дает экспоненциальный эффект на уровень безопасности!



- Что именно необходимо защитить?
- Кто, к чему и какими средствами имеет доступ?
- Каковы риски безопасности информационной системы?
- Что происходит в информационной системе?



## Уровень безопасности

## Применяемые меры безопасности

периметр

Межсетевые экраны, антивирусы для шлюзов, спам-файрволы, анализаторы контента, VPN, IPS

сеть

IDS, IPS, межсетевое экранирование, сканеры безопасности (VA), аутентификация, управление доступом, управление политиками безопасности

сервер

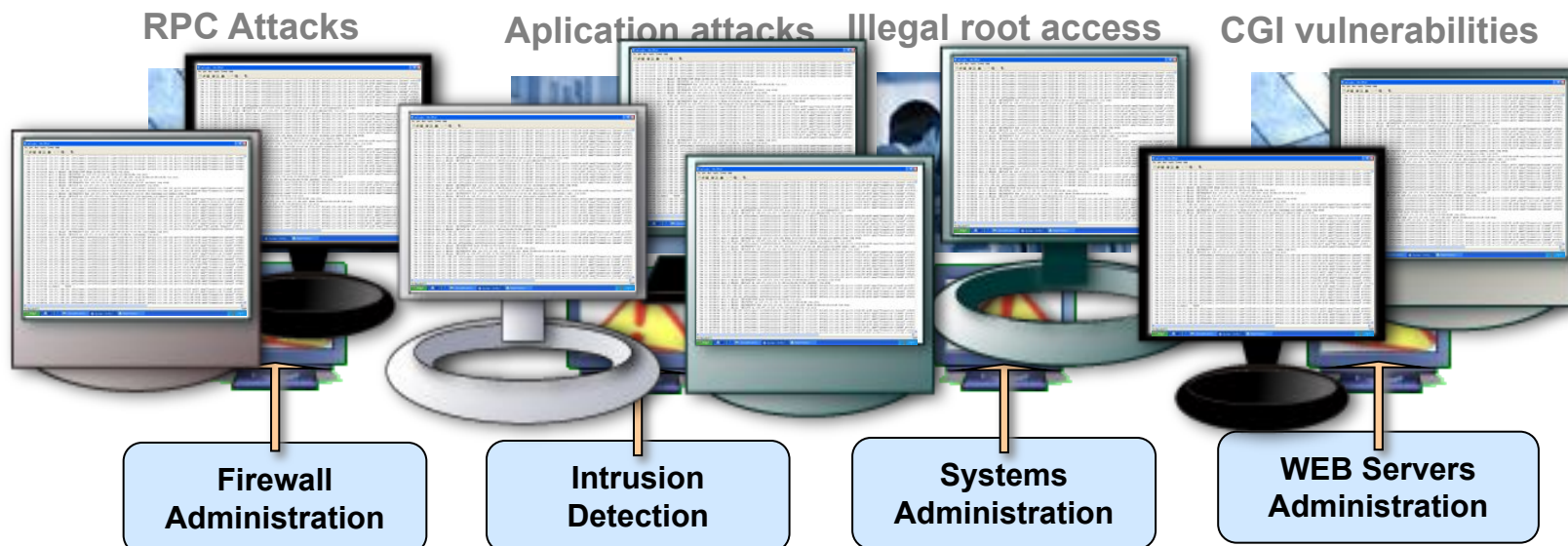
Host IDS, системные сканеры безопасности, анализаторы политик безопасности, антивирусы, управление доступом, аутентификация

приложения

Контроль ввода данных, Host IDS, анализаторы политик безопасности, антивирусы, контроль доступа, аутентификация

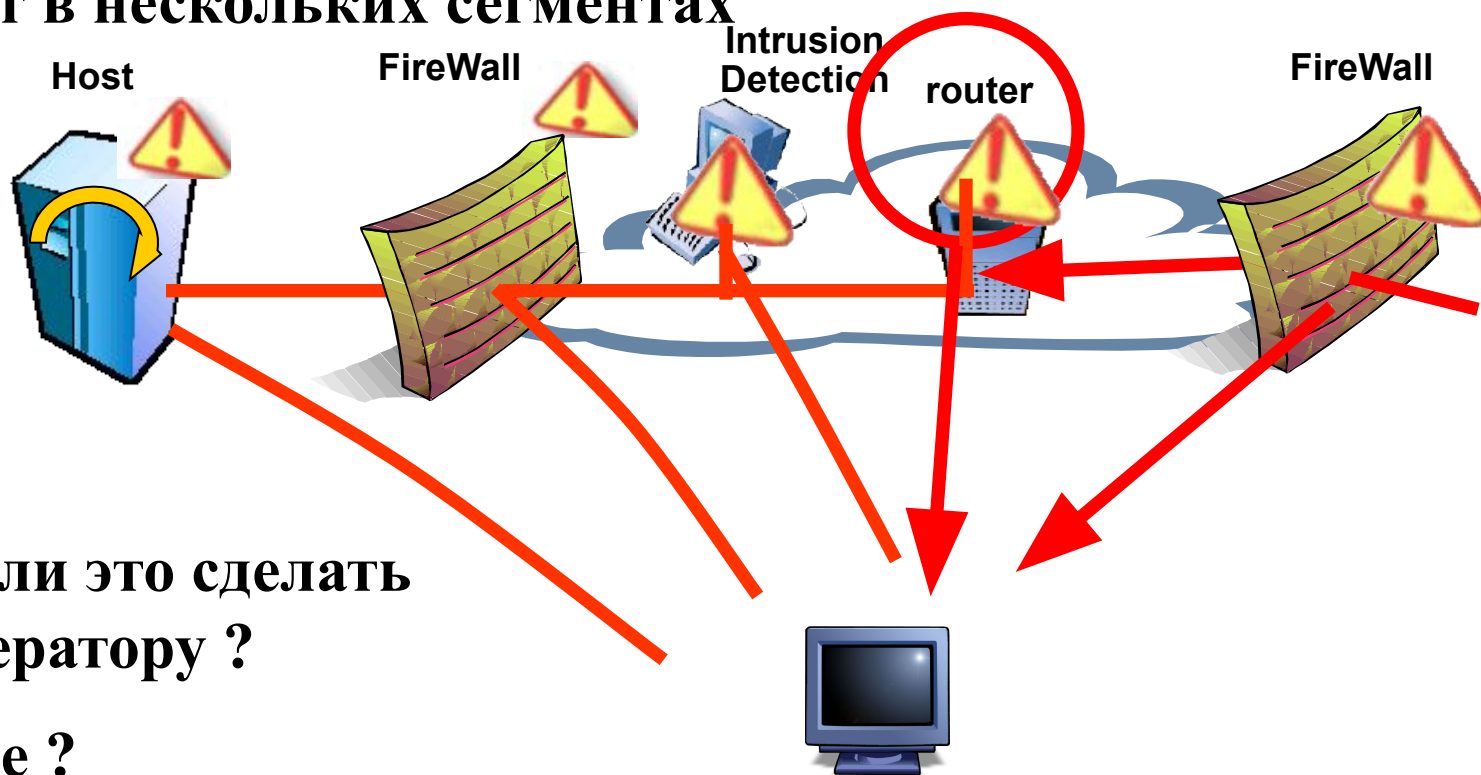
данные

Шифрование, подпись, управление доступом, аутентификация



- | **Каждый компонент видит только часть информации обрабатываемой в сети**
- | **Множество консолей:**
  - | Разные источники информации требуют определенного опыта работы с ними
- | **Нет реальной интеграции между устройствами безопасности**
  - | Смесь оборудования от различных вендоров и отсутствие стандартизации

Для своевременного обнаружения атаки нам нужно одновременно видеть **в реальном режиме времени** что происходит в нескольких сегментах

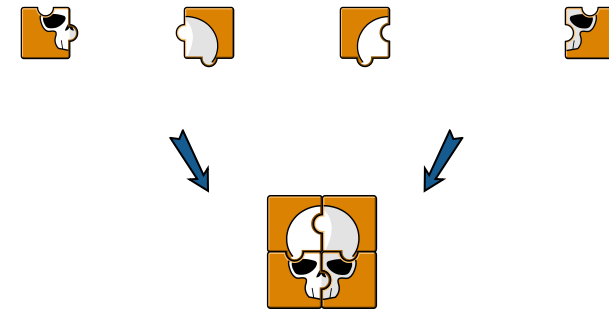


Возможно ли это сделать  
одному оператору ?

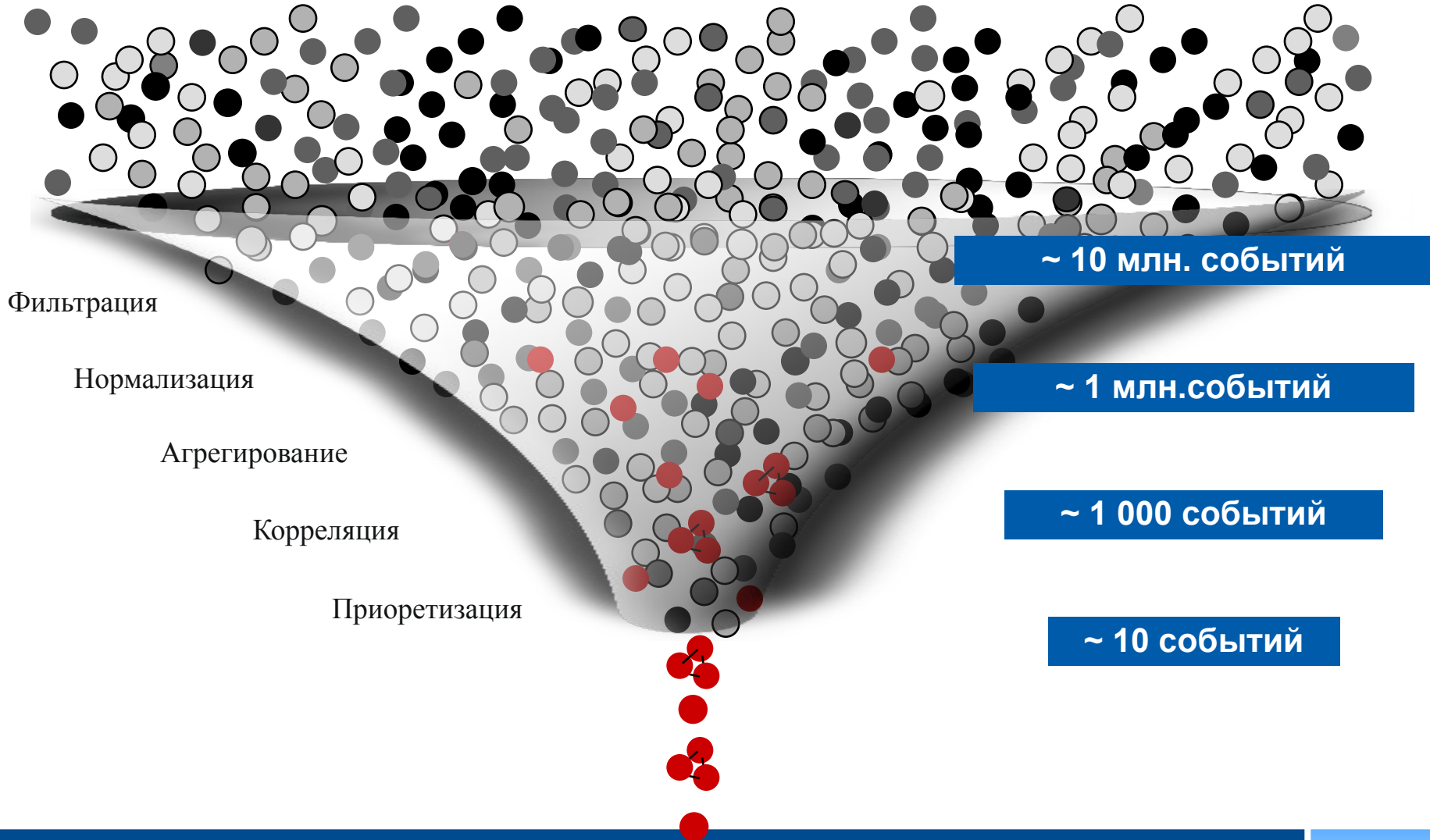
Или группе ?

МОНИТОРИНГ

- Позволяет в реальном режиме времени получать события от различных систем безопасности и, обрабатывая данные события по задаваемым правилам, определять злонамеренные воздействия, даже если они не определяются другими средствами безопасности
- Позволяет обеспечить визуализацию происходящих изменений в сети, показывая как развивалось то или иное событие или атака
- Позволяет провести расследование событий безопасности (прокрутить события назад и восстановить картину инцидента) и таким образом быстро в реальном режиме времени определить источник атаки
- Позволяет выполнять анализ соответствия текущего состояния системы безопасности заданной политике безопасности и сигнализировать о нарушениях в реальном времени
- Позволяет совместно с другими средствами безопасности пресекать нарушения в реальном режиме времени



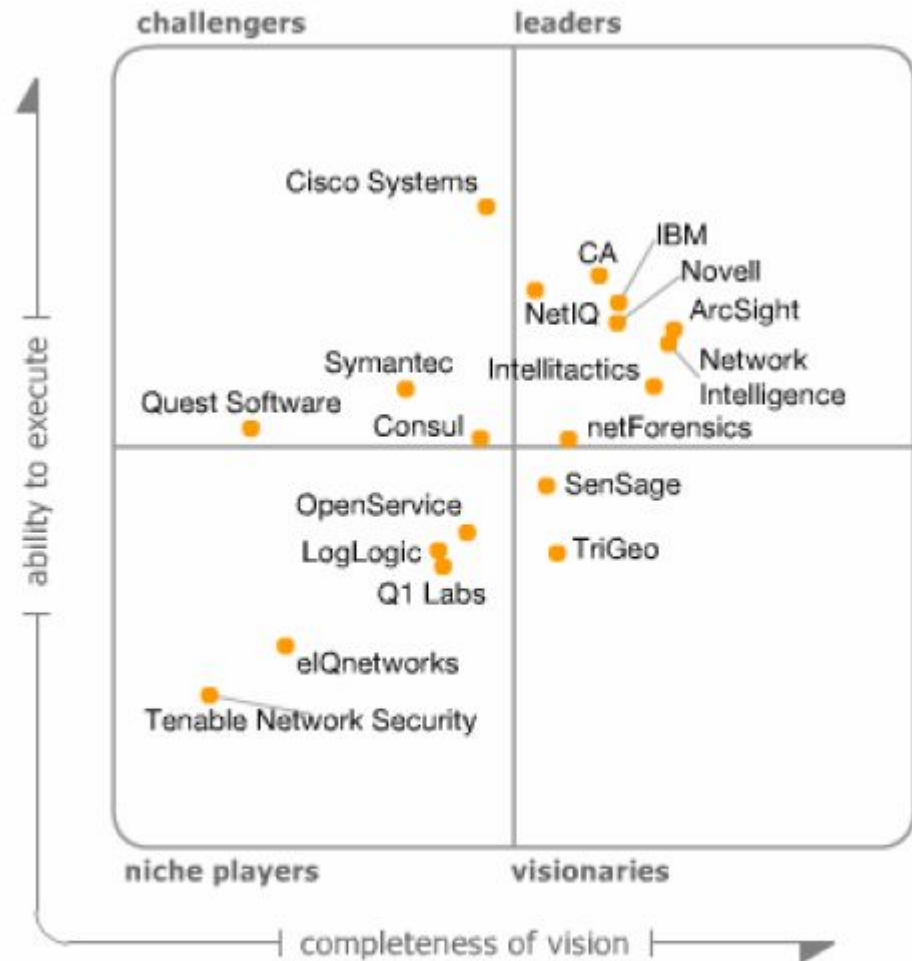
# Принцип работы полноценной SIM (SEM)



- Покупается хорошо раскрученный продукт, который, как оказывается, не поддерживает большую часть имеющегося у данной компании оборудования
- Покупается только базовый модуль, обладающий только основной функциональностью
- Не правильно позиционирован продукт - покупался продукт мониторинга сетей для мониторинга безопасности сетей.....
- Предполагалось, что есть универсальный агент или подсистема, позволяющая легко подключить не описанное в списке поддерживаемого оборудования устройство, но на практике .....

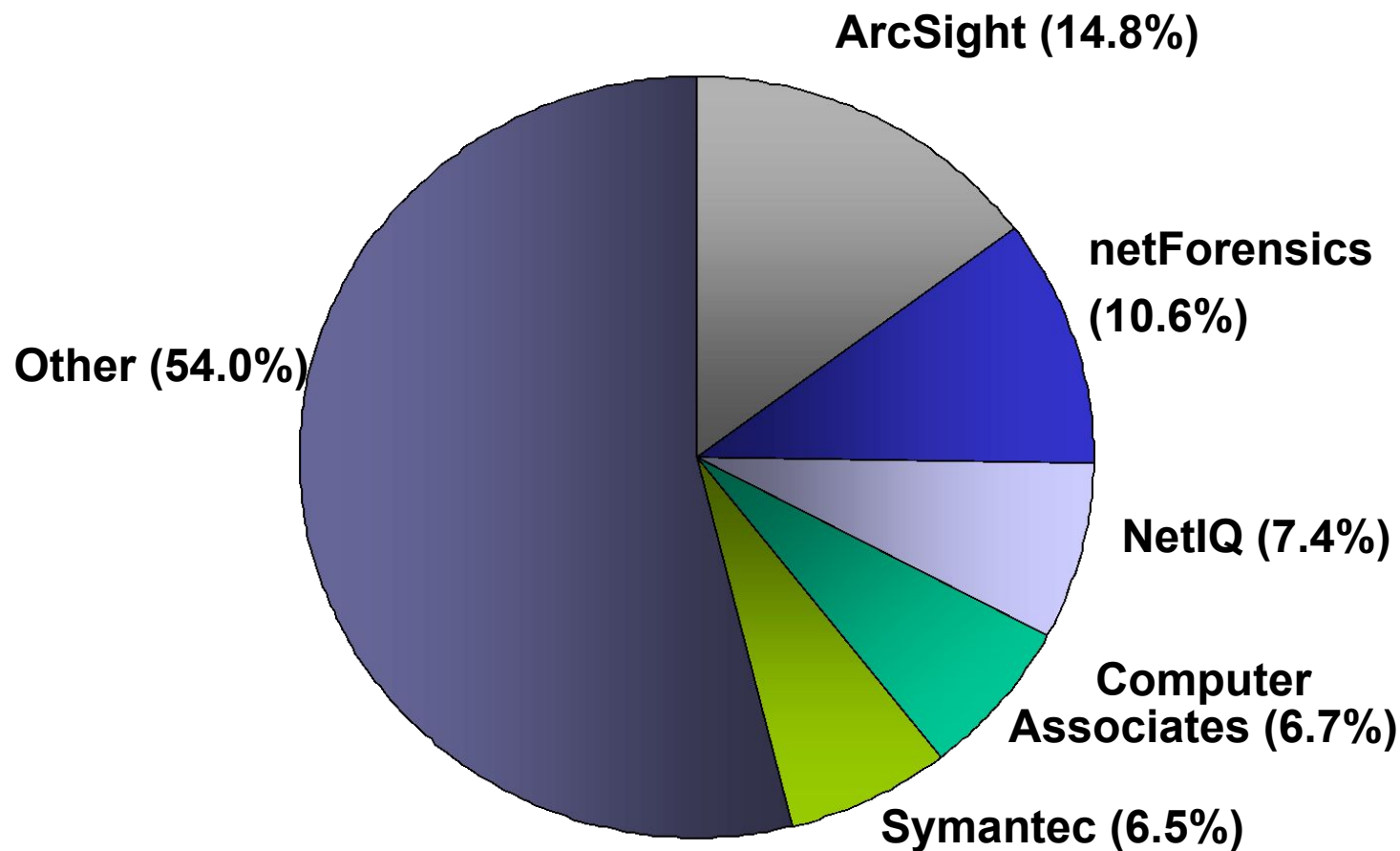
# Какие системы существуют?

- **Quest Software**
- **GuardedNet (IBM)**
- **Intelligence**
- **ISS**
- **NetForensics (SIMS)**
- **OPEN Service**
- **Protego (CISCO MARS)**
- **Symantec**
- **IBM Tivoli**
- **ArcSight**
- и другие



As of 7 May 2006

Source: Gartner (May 2006)



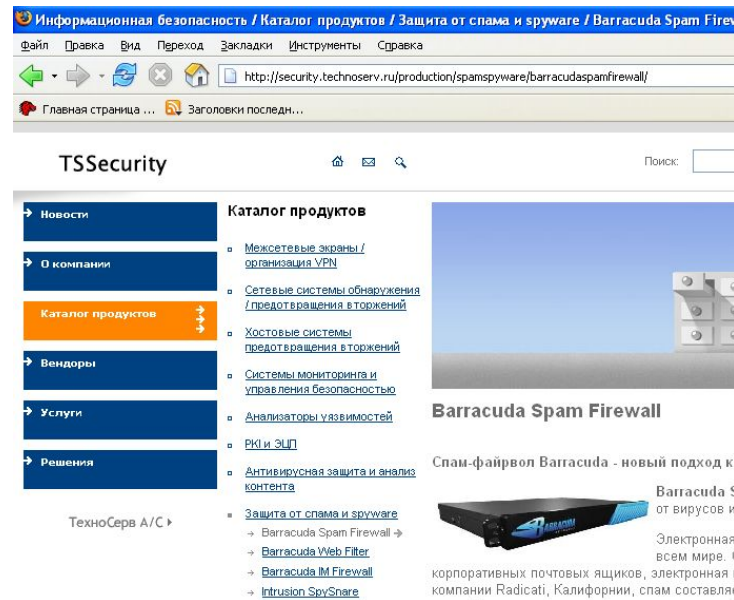
Source: IDC, 12/2005

Total = \$209.9M



## Специализированный WEB-ресурс по Информационной безопасности:

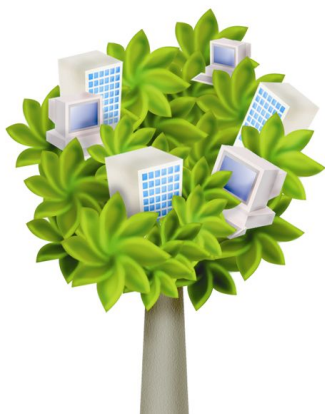
[www.SECURITY.TECHNOSERV.ru](http://www.SECURITY.TECHNOSERV.ru)



The screenshot shows a web browser window with the URL <http://security.technoserv.ru/production/spamspyware/barracudaspamfirewall/>. The page title is "Информационная безопасность / Каталог продуктов / Защита от спама и spyware / Barracuda Spam Firewall". The website layout includes a navigation menu on the left with categories like "Новости", "О компании", "Каталог продуктов", "Вендоры", "Услуги", and "Решения". The main content area is titled "Каталог продуктов" and lists various security solutions such as "Межсетевые экраны / организация VPN", "Сетевые системы обнаружения / предотвращения вторжений", "Хостовые системы предотвращения вторжений", "Системы мониторинга и управления безопасностью", "Анализаторы уязвимостей", "PKI и ЭЦП", "Антивирусная защита и анализ контента", and "Защита от спама и spyware". The "Защита от спама и spyware" category is expanded, showing sub-items: "Barracuda Spam Firewall", "Barracuda Web Filter", "Barracuda IM Firewall", and "Intrusion SpyShare". On the right side, there is a section for "Barracuda Spam Firewall" with a product image and a brief description: "Спам-файрвол Barracuda - новый подход к: Barracuda S от вирусов и Электронная всем мире. С корпоративных почтовых ящиков, электронная п компании Radicati, Калифорнии, спам составляе".

## Партнеры





111395 Москва, ул.Юности 13, корп. 2  
Тел. (095) 727-0989  
Факс (095) 727-0988  
WEB <http://www.technoserv.ru>  
E-mail [tsas@technoserv.ru](mailto:tsas@technoserv.ru)

