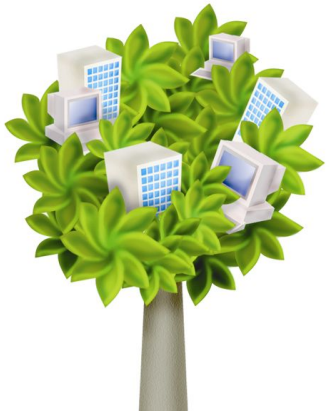
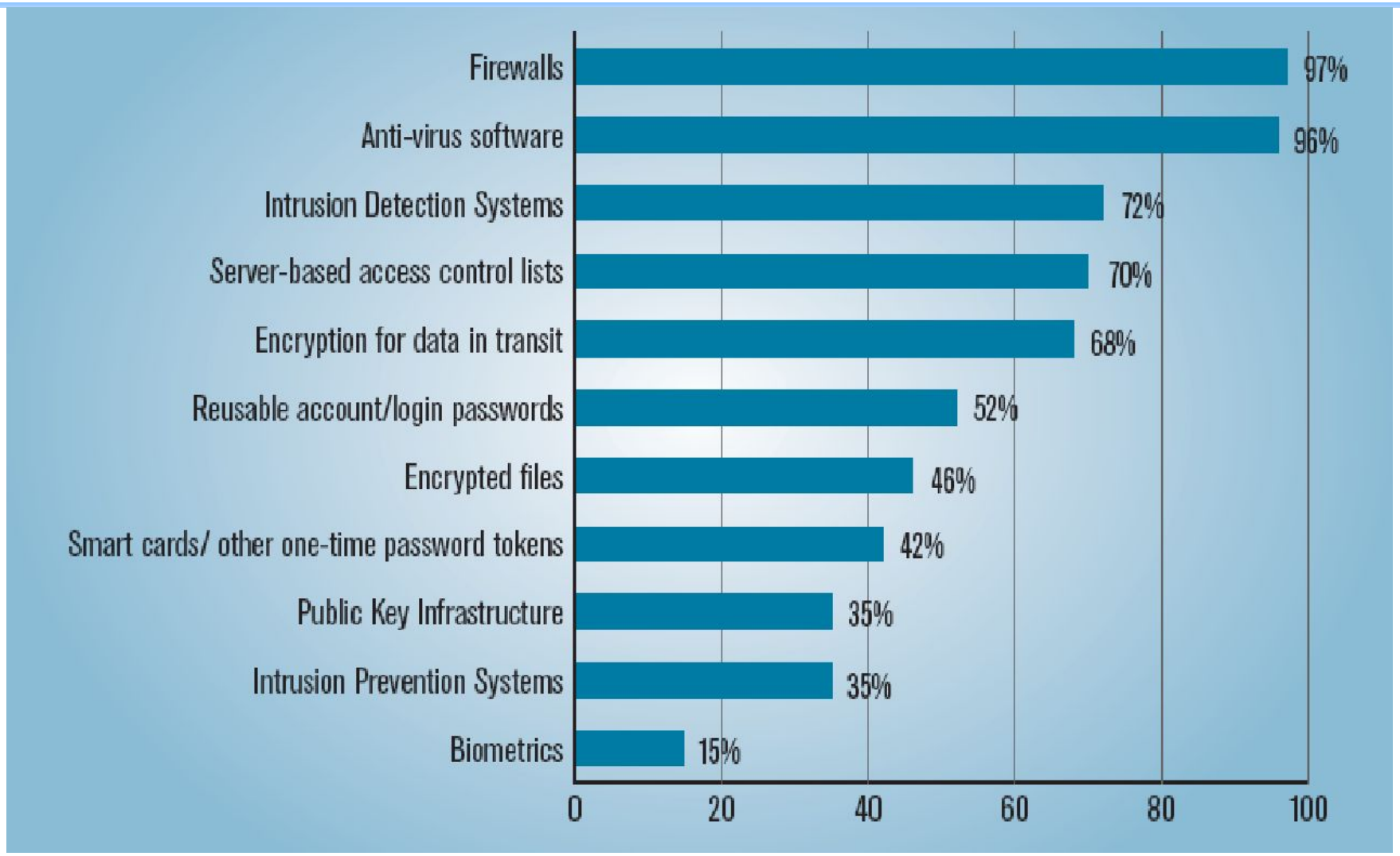
ТехноСерв А/С

Информационная безопасность - от лоскутных подходов к интегрированным и комплексным решениям



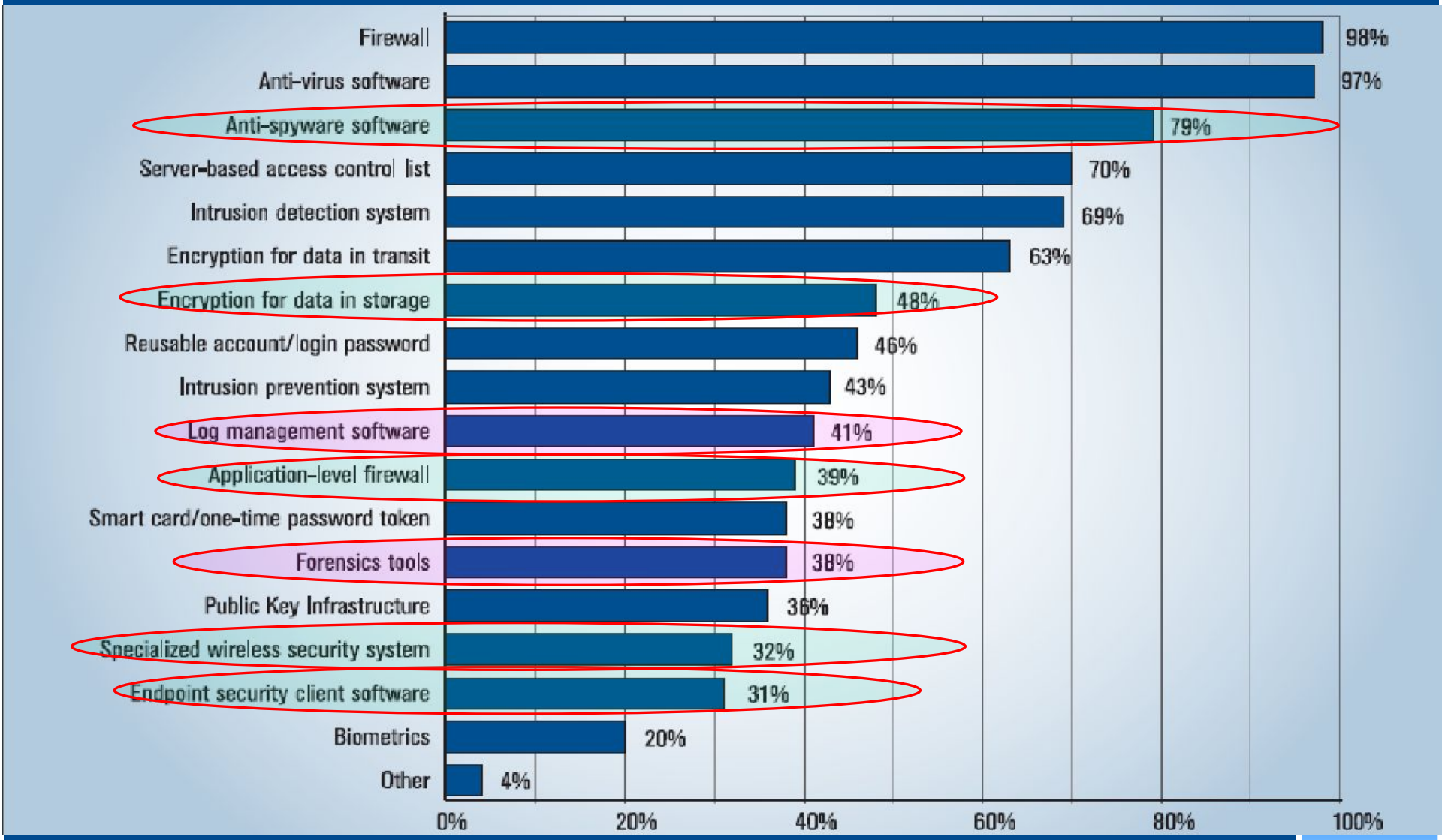
Используемые технологии в **2005** году по версии **CSI/FBI**

ТехноСерв А/С



Что используется для защиты информации в **2006** году

ТехноСерв А/С



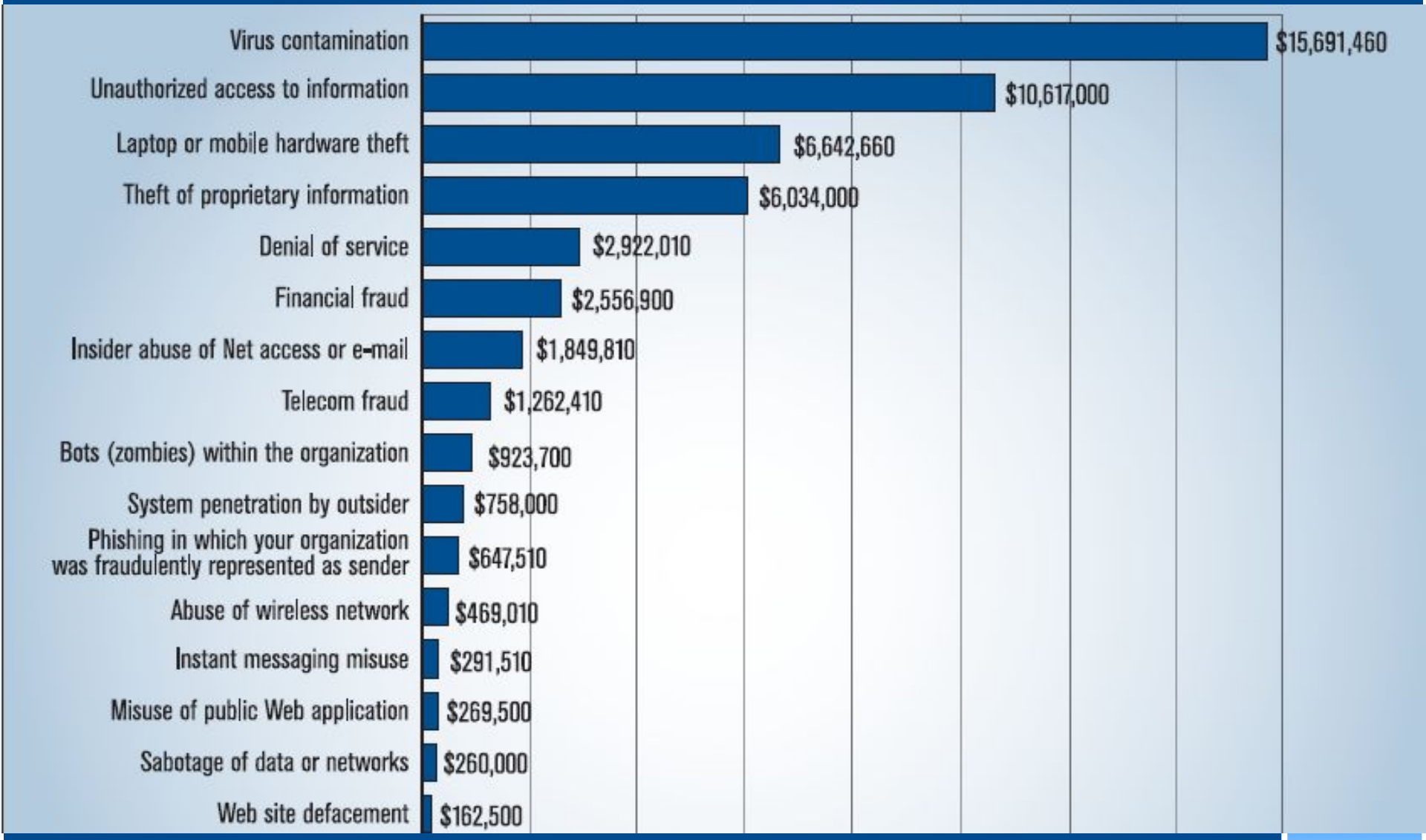
Источник: CSI/FBI 2006 год

Основные тенденции

ТехноСерв А/С

- 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



Источник: CSI/FBI 2006 год

Современная система безопасности состоит из следующих элементов:

ТехноСерв А/С

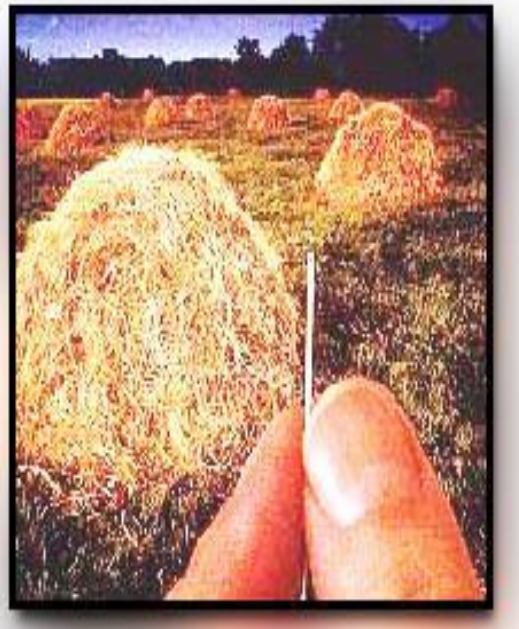
- Подсистема межсетевого экранирования и создания **VPN**
- Подсистема обнаружения сетевых вторжений
- **Host based** система предотвращения вторжений к серверам
- Подсистема антивирусной защиты
- Подсистема аутентификации и авторизации пользователей**,** разграничения доступа пользователей к ресурсам 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

Проблемы многоуровневой безопасности

ТехноСерв А/С

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

Все это дает экспоненциальный эффект на уровень безопасности!



Построение безопасности начинается с вопросов о том:

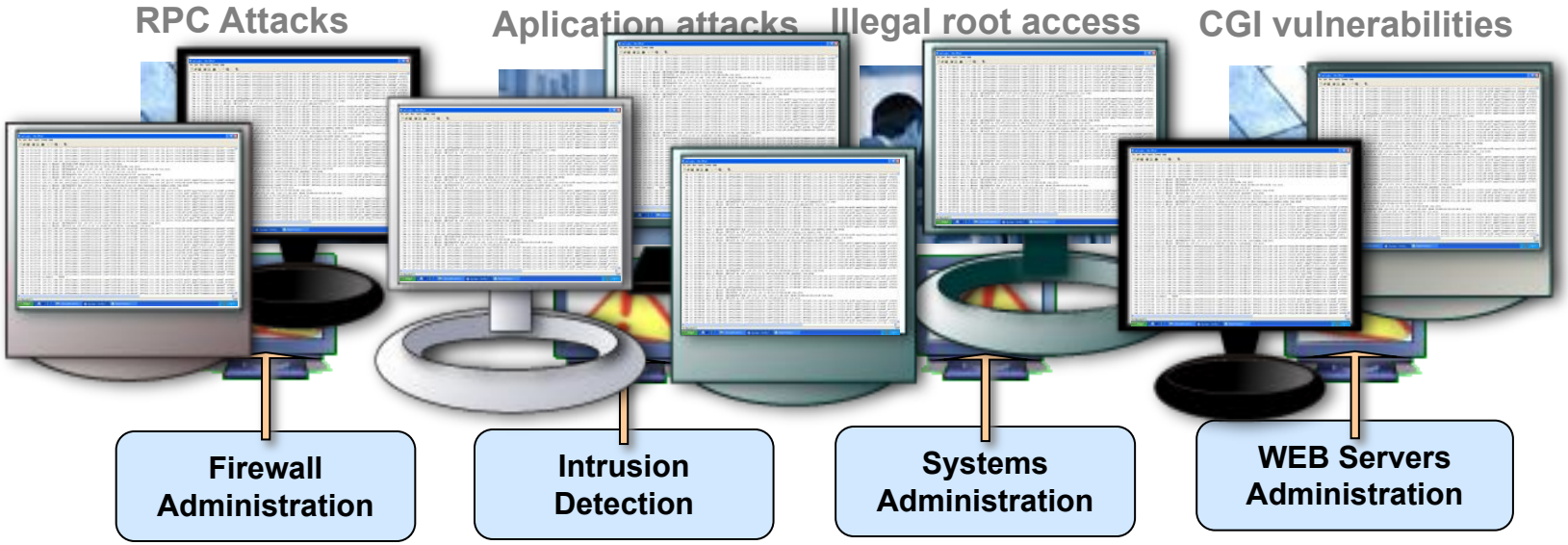
- Что именно необходимо защитить?
- Кто, к чему и какими средствами имеет доступ?
- Каковы риски безопасности информационной системы?
- Что происходит в информационной системе?

Уровни защиты

ТехноСерв А/С

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

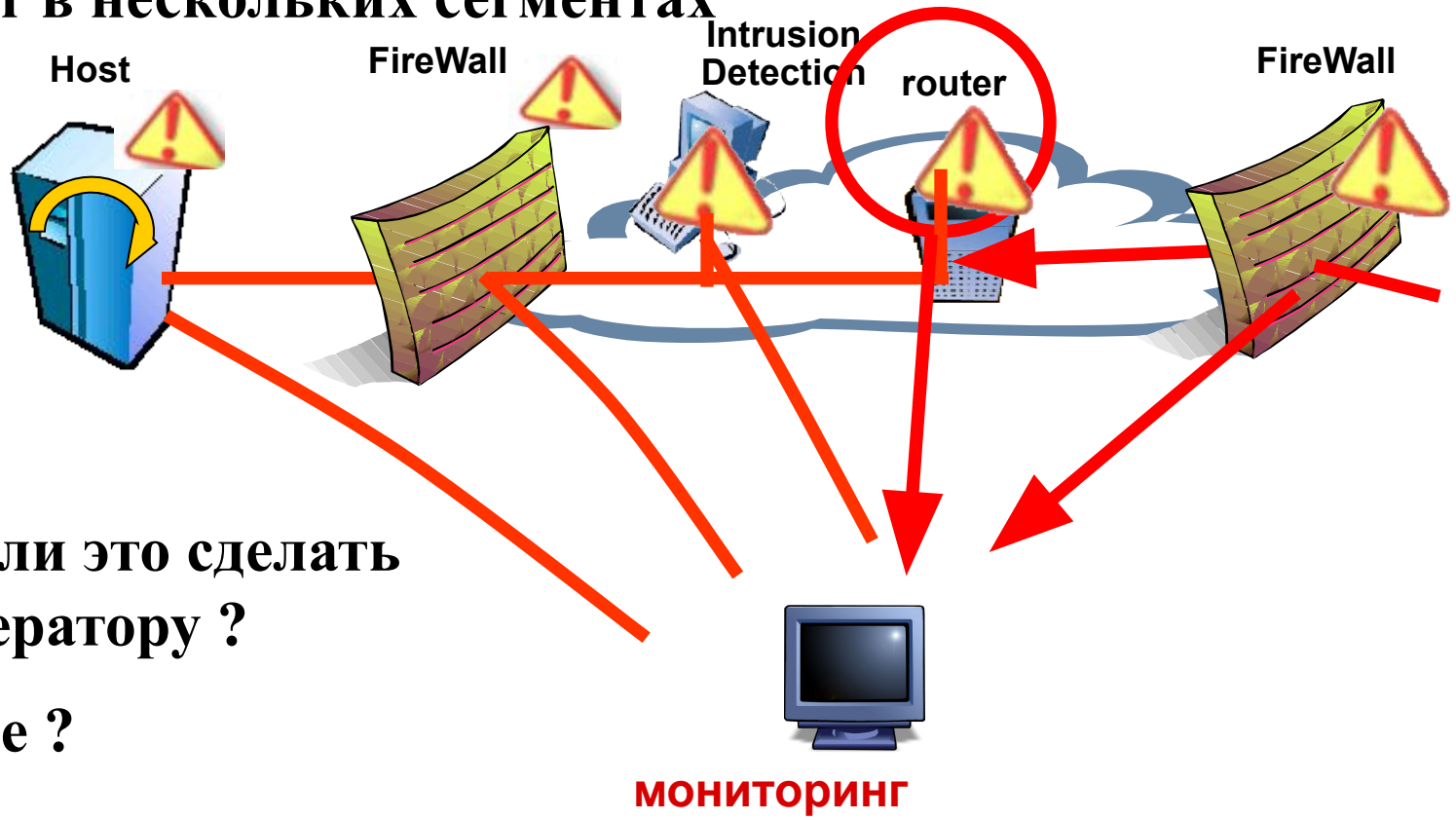
Проблемы многоуровневой безопасности



- **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

Мониторинг атаки

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



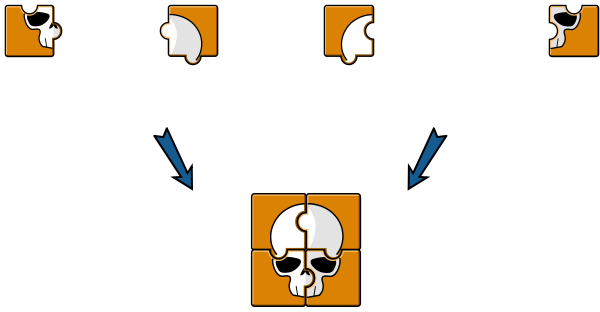
Возможно ли это сделать одному оператору ?

Или группе ?

Система анализа, корреляции и управления информационной безопасностью

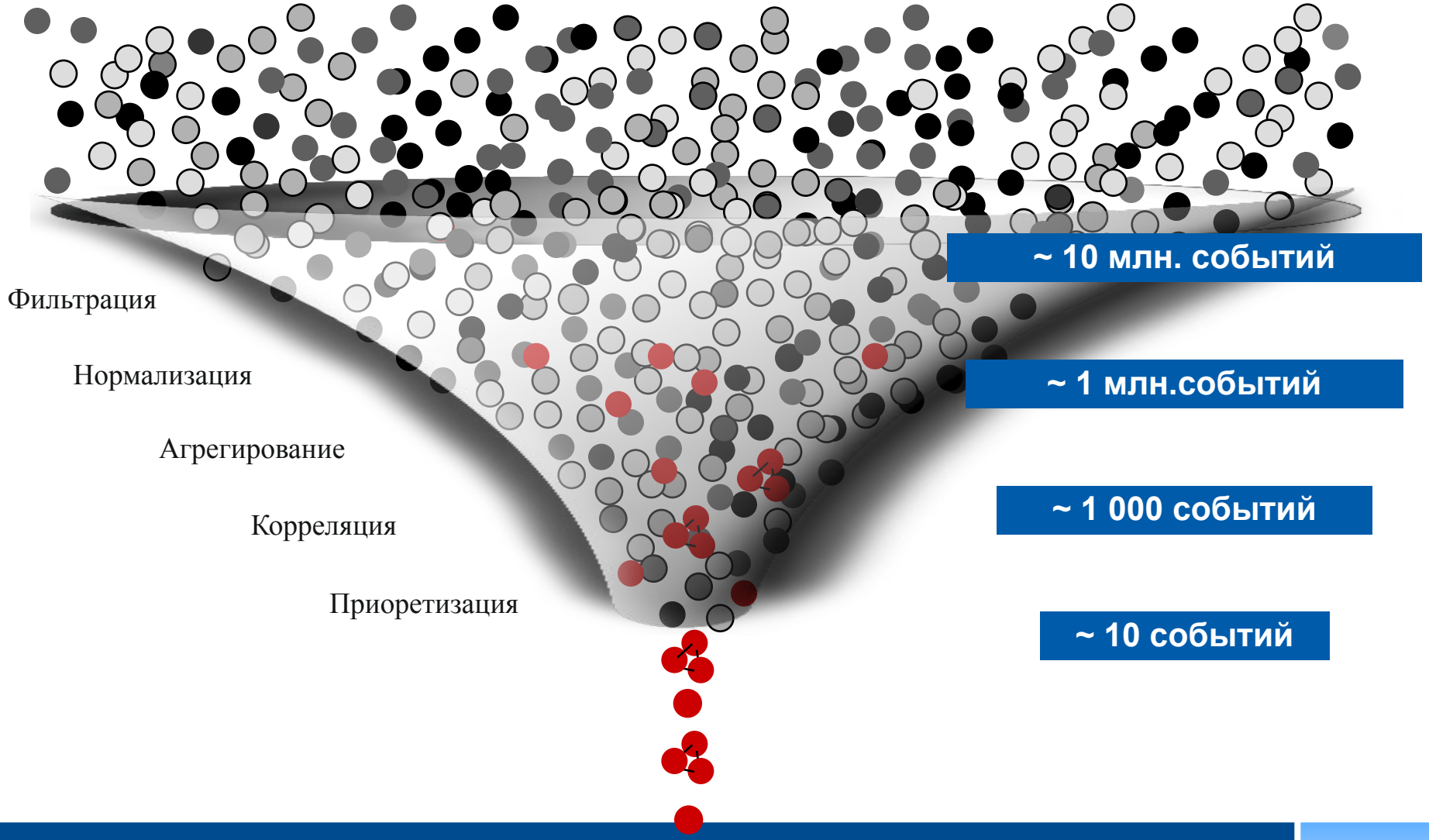
ТехноСерв А/С

- 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)**

ТехноСерв А/С



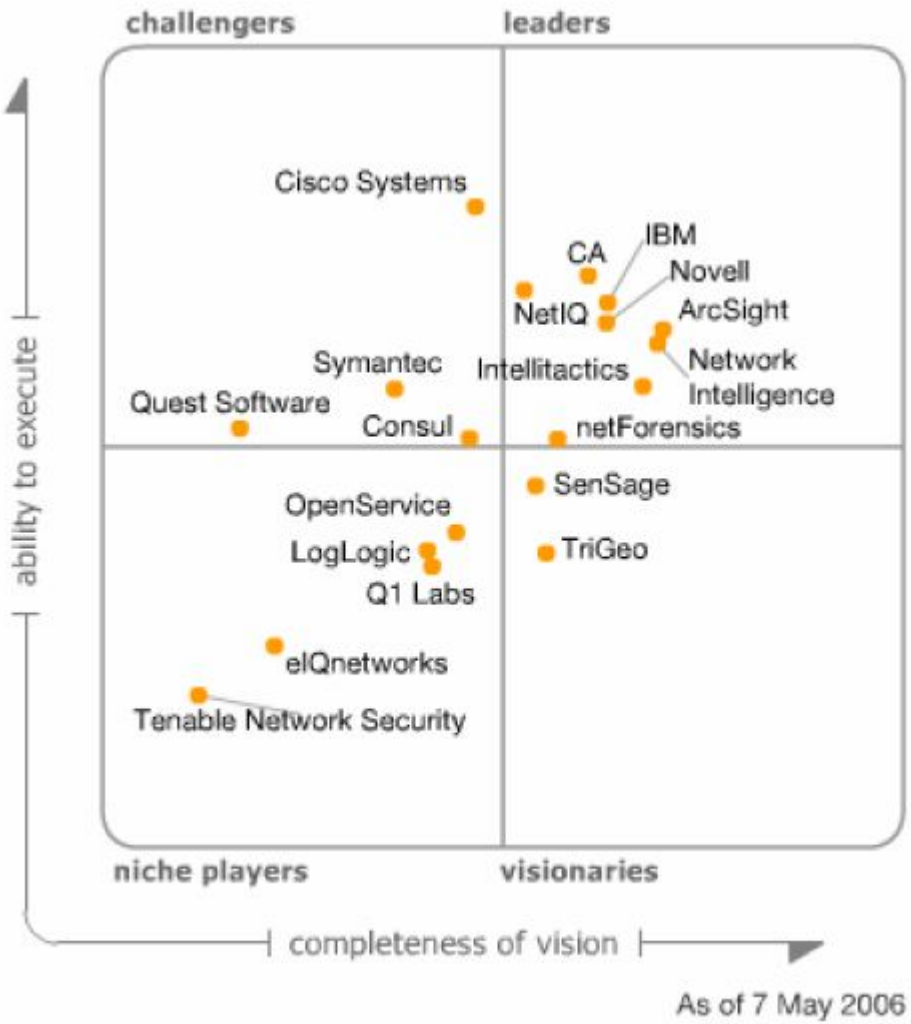
Основные ошибки при выборе и покупке систем **SIM (SEM)**

ТехноСерв А/С

- 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 .....

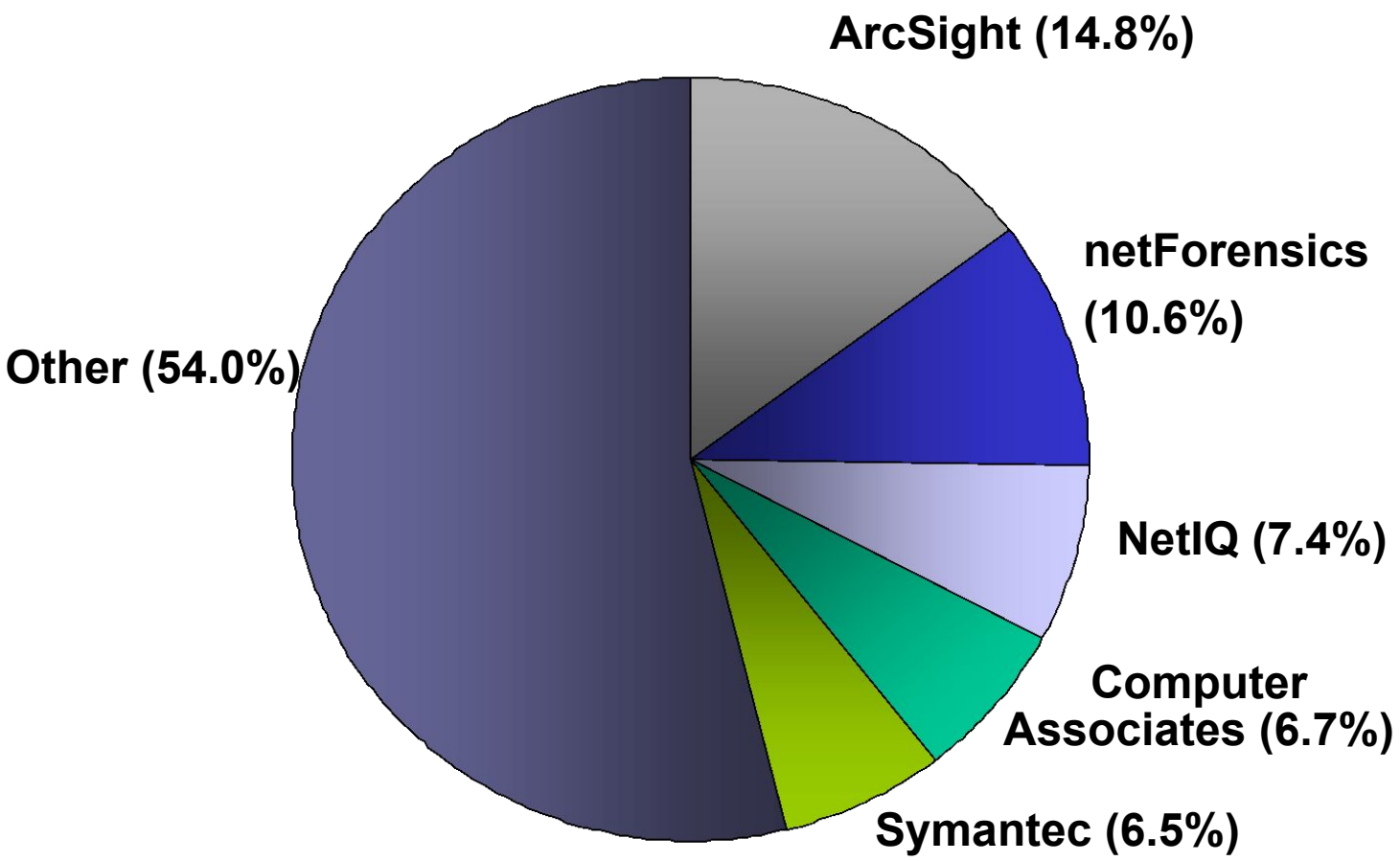
Какие системы существуют?

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



Source: Gartner (May 2006)

С точки зрения рынка



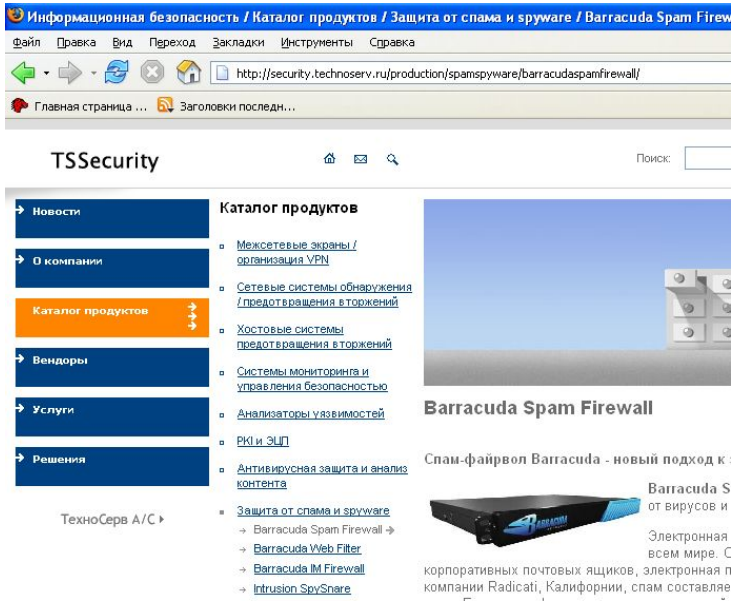
Source: IDC, 12/2005

Total = $209.9M

ТехноСерв А/С

Специализированный WEB-ресурс по Информационной безопасности:

www.SECURITY.TECHNOSERV.ru



ТехноСерв А/С

Партнеры

BSi Management Systems

StoneGate™ STONEGATE SECURITY PLATFORM FW VPN IPS FOR SECURITY AND CONTINUITY

CISCO SYSTEMS

NET SCREEN® Scalable Security Solutions

ORACLE® Enabling the Information Age

BARRACUDA NETWORKS

ArcSight

symantec™

INTRUSION

s•terra csp

SECP•INT®

QUALYS® ON DEMAND SECURITY

ТехноСерв А/С

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