



[www.atlas.ua](http://www.atlas.ua)

# Управление рисками и контроль выполнения политики безопасности с помощью системы IP-Guard

**Виктор Жора,  
Начальник отдела защиты информации  
АОЗТ «Атлас»**

# Актуальные вопросы ИТ-безопасности в компаниях



# Типичные проблемы ИТ



Игры · Биржи ·  
Чаты

Веб-серфинг · Печать личных док-тов

Онлайн-видео · Радио · Музыкак

Невозможно удаленно решить проблему

Невозможно отслеживать изменения

Загрузка администраторов

# Система управления IP-guard

Преимущества  
IP-guard

→ Защита информации

→ Разграничение доступа

→ Планирование ресурсов

→ Контроль данных

# Различные модули для различных целей защиты

Управление доступом к файлам

Управление печатью

Управление устройствами

Контроль сети

Управление ПО

Управление веб-доступом

Управление почтой

Управление Instant Message

Снимки экранов

Управление полосой пропускания

Управление активами

Удаленное управление

Управление съемными носителями

Базовая информация

# Управление файловыми операциями

- Журнал операций с файлами

Регистрация операций с файлами, включая  
create, access, edit, copy, move, delete

Регистрация операций с файлами на съемных носителях и в сетевых папках

Регистрация операций с файлами в папках общего доступа других компьютеров

- Политика документов

Контроль доступа к важным документам

Предотвращение несанкционированного доступа на внешние устройства и сетевые хранилища

Резервное копирование важной информации при удалении или модификации



# Управление печатью

- Журнал печати

Регистрация информации: приложение, принтер, пользователь и имя документа

Запись количества распечатанных страниц

- Политика печати

Блокировка печати из неавторизованных приложений

Блокировка печати на выбранных принтерах



# Управление устройствами

- **Управление носителями**  
(Floppy • CD • USB • Карты памяти)
- **Управление устройствами связи**  
Контроль передачи данных по портам  
(COM • LPT • MODEM • Infrared  
• Bluetooth • Direct connection • Dialup)
- **Управление другими устройствами**  
Контроль USB-устройств, карт беспроводной связи и других устройств.





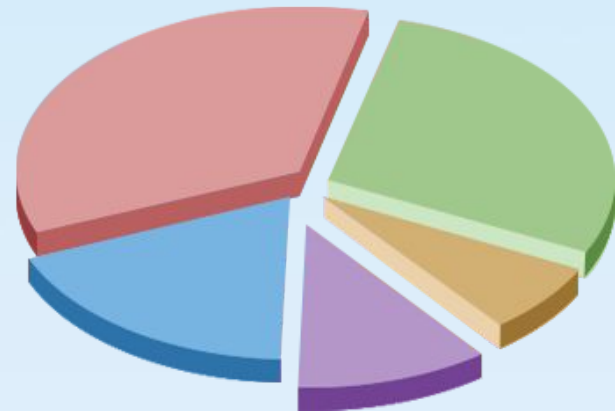
# Управление сетевым доступом

- **Управление сетевым взаимодействием**
  - Межсетевой экран для управления доступом к адресам и портам
  - Запрет использования определенных портов для взаимодействия с неавторизованными компьютерами
- **Привязка IP/MAC**
  - Запрет изменения сетевых настроек
- **Обнаружение вторжений**
  - Сканирование сети и предотвращение НСД



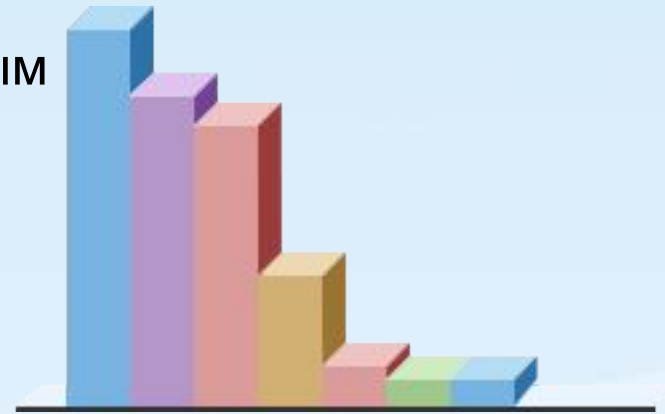
# Управление приложениями

- Журнал приложений и статистика
  - Регистрация открытия и закрытия приложений
  - Регистрация смены окон для контроля за использованием компьютеров
  - Статистика использования приложений и оценка эффективности работы персонала
- Политика приложений
  - Запрет игр и чатов
  - Борьба с вредоносным ПО



# Управление веб-доступом

- **Статистика веб**  
Общие данные о типах посещаемых сайтов
- **Журнал веб**  
Регистрация URL и заголовков
- **Политика веб**  
Блокировка веб-сайтов, не относящихся к работе  
Блокировка веб-сайтов с вредоносным контентом



# Управление почтой

- **Запись почты**

Регистрация email, webmail, почты Exchange и Lotus Notes

Запись сообщений и вложений

- **Политика почты**

Ограничение экаунтов отправителей

Блокировка определенных получателей

Блокировка почты с вложениями определенных имен и размеров



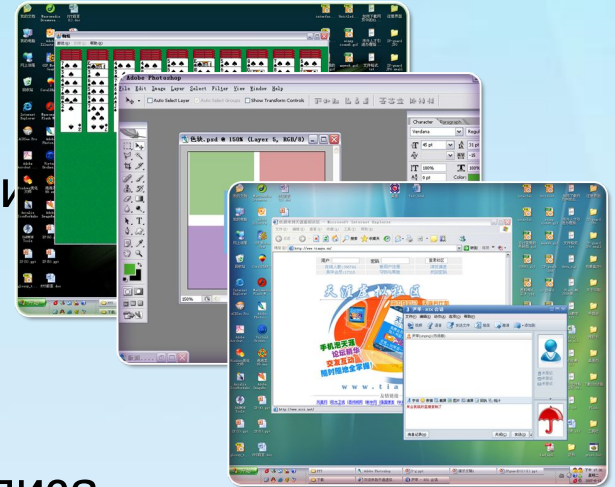
# Управление Интернет-пейджерами

- Регистрация мгновенных сообщений
  - Запись всего контента IM-сессии
- Политика файлов IM
  - Ограничение отправки файлов определенных имен и размеров
  - Резервное копирование передаваемых файлов



# Запись экранов

- **Запись в реальном времени**
  - Просмотр экранов в реальном времени
  - Поддержка нескольких мониторов
  - Мультиэкранный режим
- **История снимков экрана**
  - Запись экранов для дальнейшего анализа
  - Гибкая настройка частоты записи
  - Сжатие данных



# Управление полосой пропускания

- Статистика сетевого трафика

  - Статистика трафика по адресам

  - Статистика по портам

  - Анализ данных по  
определенным периодам времени



- Политика сетевого трафика

  - Назначение различных полос пропускания для  
различных адресов и портов

  - Предотвращение BT, P2P и программ-загрузчиков

# Управление активами

- Управление оборудованием и ПО

- Полная информация об установленном ПО и оборудовании

- Детальная история изменений

- Редактируемые свойства для добавления дополнительной информации

- Возможность добавления невычислительных активов для стандартизации инвентаризации





# Управление активами

- **Управление обновлениями**  
Агент определяет установленные пакеты продуктов Microsoft.  
Загрузка и установка патчей
- **Контроль уязвимостей**  
Сканирование на предмет уязвимостей и анализ
- **Внедрение ПО**  
Автоматическая установка, выполнение и распространение файлов  
Поддержка backend и интерактивной установки

# Удаленное управление

- **Управление в реальном времени**

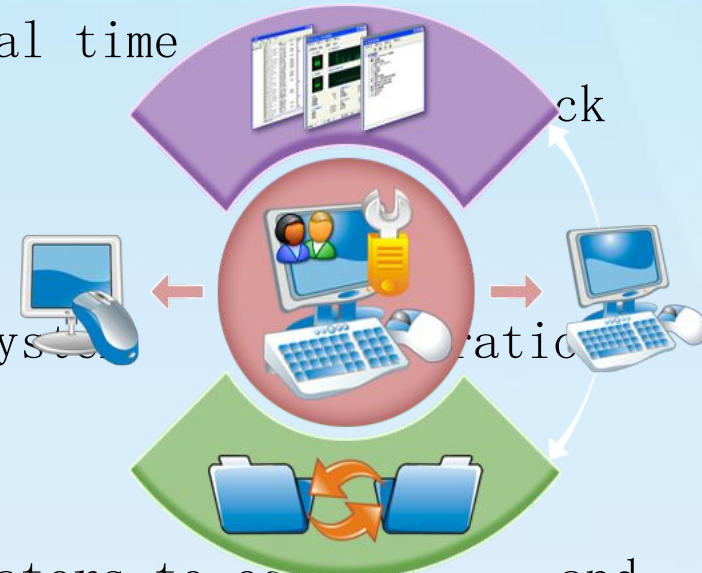
- View agents' system messages in real time
  - Remote diagnostic agent's problems
  - system status

- **Remote Control**

- Easy assist users and demonstrate systems
  - to users

- **Remote File Transfer**

- Remote file transfer help administrators to collect and
  - update files more efficiently



# Removable Storage Management

- **Endpoint Devices Authorization**

Define removable storage access rights.

Prevent unauthorized removable device's illegal access to agent computers.

- **Endpoint Devices Encryption**

Encrypt documents on specific removable storage devices.

Prevent illegal access to encrypted documents.

# New Features

Multi-Language

Support Multi-Language for multi-national corporation

Easy Management

Can be managed by computer or by user. Each with multi-level grouping and audit trail

Flexible Policy

Policies are set with combination of group inherited policy, normal policy, and offline policy

Classes System

Custom defined classes to be used throughout the system

# Information Security Solution

Confidential information such as source codes, chemical formulas, and design blue prints are saved in documents. Therefore, document security is the core of information security.

- Monitor document operations
- Block information leak from movable devices and network shares
- Block information leak by external devices
- Block information leak from Internet
- Prevent illegal computers to access the internal network to steal data
- Enhance security by encryption



# Behavior Management Solution

Monitor and control computer usage of employees. Plan network resources accordingly to ensure company resources are effectively used.

- **Behavior Control**

Application • Website • Event Log

- **Network Control**

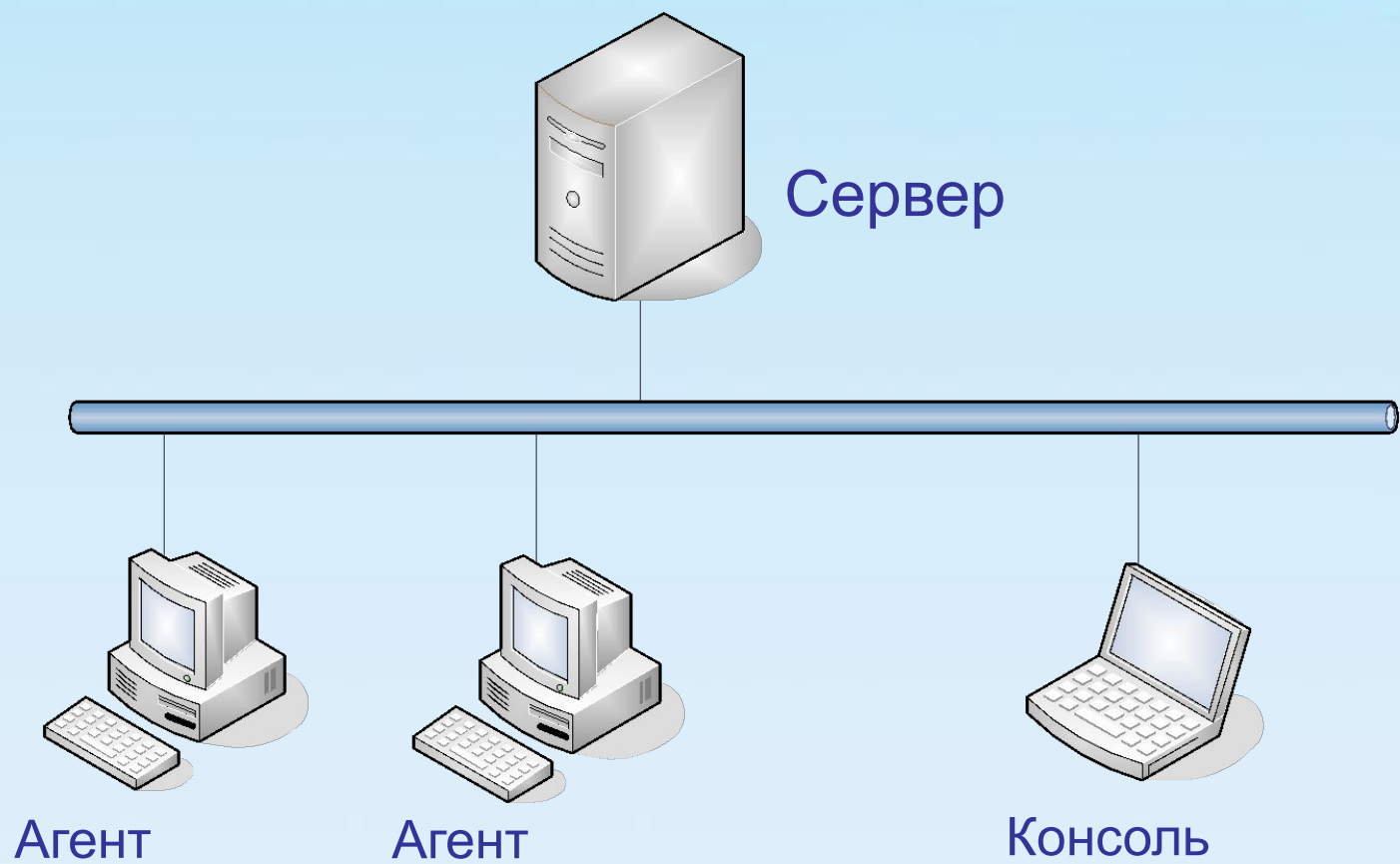
Flow Control • Communication Control

- **Content Control**

Mail • Instant Message • Screen Snapshot



# Базовая архитектура



# Минимальные требования

## Агент

- Pentium III 500
- 128MB Memory
- 1G HDD
- OS
  - Win9x / NT4
  - Win2000 / XP
  - Win2003

## Консоль

- Pentium III 1G
- 256MB Memory
- 4G HDD
- OS
  - Win2000 / XP
  - Win2003

## Сервер

- Pentium 4 2G
- 512MB Memory
- 50GB HDD
- OS
  - Win2000 SP4 / XP SP2
  - Win2003 SP1
- Database
  - SQL Server 2000 SP4 /
  - 2005 SP1 / MSDE /
  - 2005 Express





Благодарю за внимание

**[www.atlas.ua](http://www.atlas.ua)**