



# Политика безопасности компании I-TEAM

---

## **IT-DEPARTMENT**

Подготовил:

**Загинайлов Константин Сергеевич**



# Средства защиты информации для компании I-TEAM

---

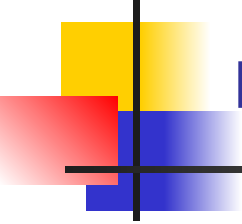
- средства управления обновлениями программных компонентов
- межсетевое экранирование;
- построения VPN;
- контроля доступа;
- обнаружения вторжений и аномалий;
- резервного копирования и архивирования;
- предотвращения вторжений на уровне серверов;
- аудита и мониторинга средств безопасности;
- контроля деятельности сотрудников в сети Интернет;
- анализа содержимого почтовых сообщений;
- анализа защищенности информационных систем;
- защиты от спама;
- защиты от атак;
- контроля целостности;
- инфраструктура открытых ключей;
- усиленной аутентификации



# Средства защиты информации для компании I-TEAM

---

- **средства управления обновлениями программных компонентов**
- **межсетевое экранирование;**
- **построения VPN;**
- **контроля доступа;**
- **обнаружения вторжений и аномалий;**
- **резервного копирования и архивирования;**
- **предотвращения вторжений на уровне серверов**



# Средства управления обновлениями программных компонентов

---

- Microsoft Software Update Services
- Становится возможным организовать и контролировать необходимые обновления программных компонентов с одной точки.
- При этом предприятие получает следующие преимущества.



# Преимущества

---

- увеличивается надежность функционирования программных компонентов
- уменьшается время на техническую поддержку и сопровождение программных компонентов
- повышается защищенность систем в целом, в частности, уменьшается количество инцидентов, связанных с вирусами и враждебными апплетами.



# Межсетевое экранирование

---

- Межсетевые экраны (брандмауэры) используются как средства защиты от несанкционированного доступа периметра сети.
- Пример: ZoneAlarm Pro (Zone Labs)



# VPN

---

- Средства построения виртуальных частных сетей, VPN, используются для организации защиты трафика данных, передаваемых по открытым каналам связи.

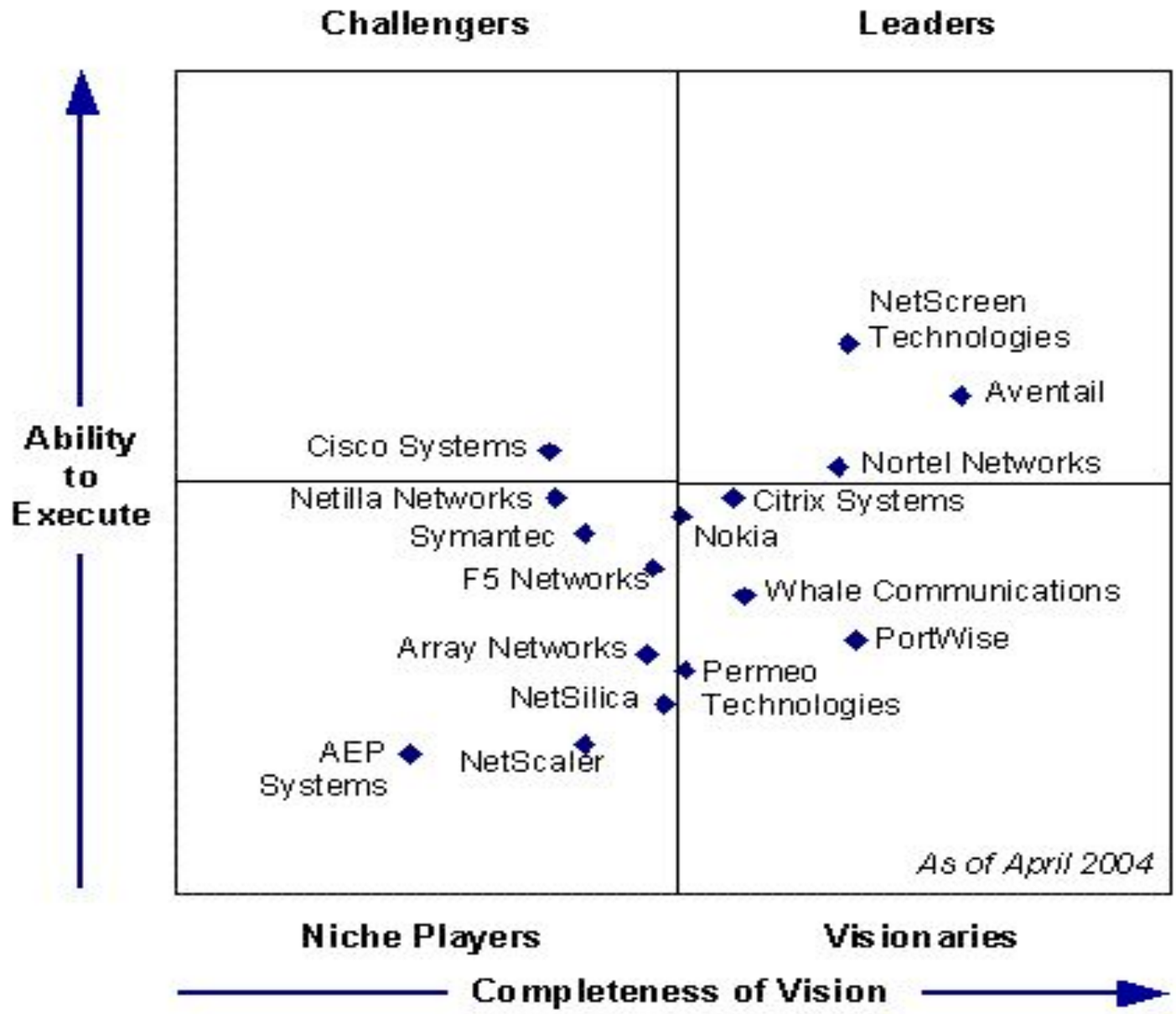
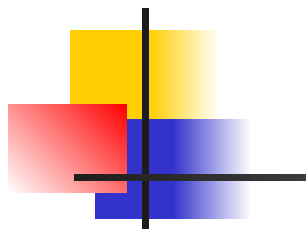
# При этом защита организуется:



---

- на физическом уровне (защита кабелей, экранизация наводок),
- на сетевом уровне (например, шифрование трафика от компьютера до компьютера на основе протокола IPsec),
- на транспортном уровне (например, шифрование данных, передаваемых одним приложением другому (на другом компьютере) на основе протокола SSL),
- на прикладном уровне (например, шифрование данных приложением самостоятельно).







# Контроль доступа

---

- Появление средств контроля доступа обусловлено необходимостью регламентировать доступ множества пользователей к приложениям и информационным ресурсам компании. Данные средства осуществляют аутентификацию (точное опознание) подключающихся пользователей и процессов, авторизацию (наделение определенными полномочиями) пользователей и процессов.
- Пример: OBLIX



# Средства обнаружения вторжений и аномалий

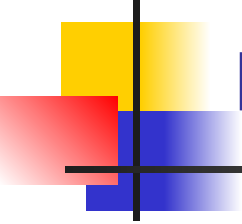
---

- Средства обнаружения вторжений, IDS (*Intrusion Detection Systems*) и аномалий позволяют с помощью некоторого регламента проверок контролировать состояние безопасности корпоративной сети в реальном масштабе времени.

# Magic Quadrant for Intrusion Detection Systems, 2H03



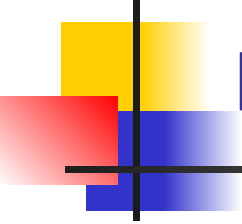
Source: Gartner Research (April 2004)



# Средства резервного копирования и архивирования

---

- Средства резервного копирования и архивирования применяются для обеспечения целостности хранилищ данных в случаях аппаратных и программных сбоев, ошибочных действий администраторов и пользователей
- Лидеры: Veritas NBU, IBM, Legato



# Средства предотвращения вторжений на уровне серверов

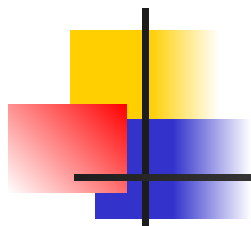
---

- Так как сервера компании обычно являются основной целью атак злоумышленников (на них обрабатывается основная часть конфиденциальной информации компании), то необходимо использовать средства предотвращения вторжений на уровне серверов
- Пример: Cisco Security Agent

# Magic Quadrant for Intrusion Detection Systems, 2H03



Source: Gartner Research (April 2004)



**Продолжение следует >>>**  
**Спасибо за внимание!**