# Защита от угроз, передаваемых в шифрованном трафике

eSafe®

**ОРГАНИЗАТОРЫ**



Руководитель направления
контент-безопасности
Владимир Бычек

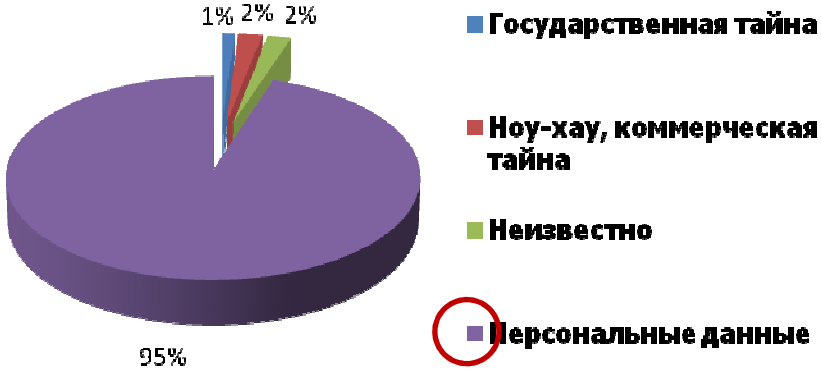
v.bychek@aladdin.ru

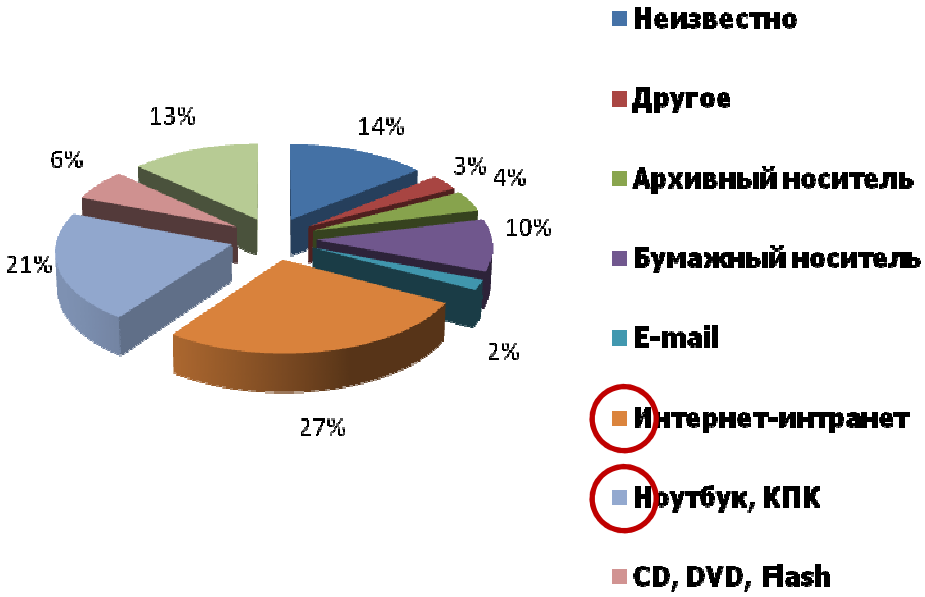
5-6 ноября 2008

# Есть ли противопоставление?

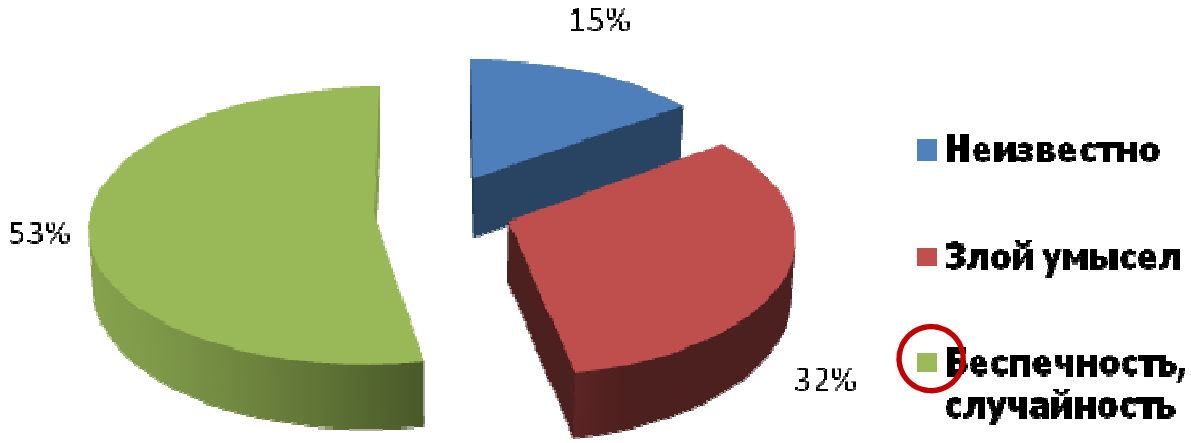
**DLP vs. CF**

# Объект и каналы утечек I/2008



# Причины утечек I/2008



# Причины утечек I/2008

- Большая часть утечек происходит неумышленно. Перекрыть возможности случайной утечки означает решить проблему на три четверти. Борьба же с инсайдерами-злоумышленниками – это в среднем менее приоритетная и более сложная задача. При ограниченности средств её следует решать во вторую очередь.
- Мобильные носители информации (ноутбуки, флэшки и т.п.) и Интернет – это два основных канала утечек. Как намеренных, так и случайных. “Мобильные” ненамеренные утечки достаточно легко перекрыть, введя обязательное шифрование данных.

# СКРЫТЫЕ И НЕКОНТРОЛИРУЕМЫЕ КАНАЛЫ

# Схема включения

# Нелегитимные коммуникации

**Нелегитимные коммуникации**

- HTTP PROXY 13,531
- SOCKS PROXY 57
- ANONYMUS WEB-PROXY 1,791
- MS INTERNET NET SHARING 3
- HTTP Tunneling 5
- HTTP (SSL) Tunneling 48
- HTTP OVER SSL (HTTPS) 1,502

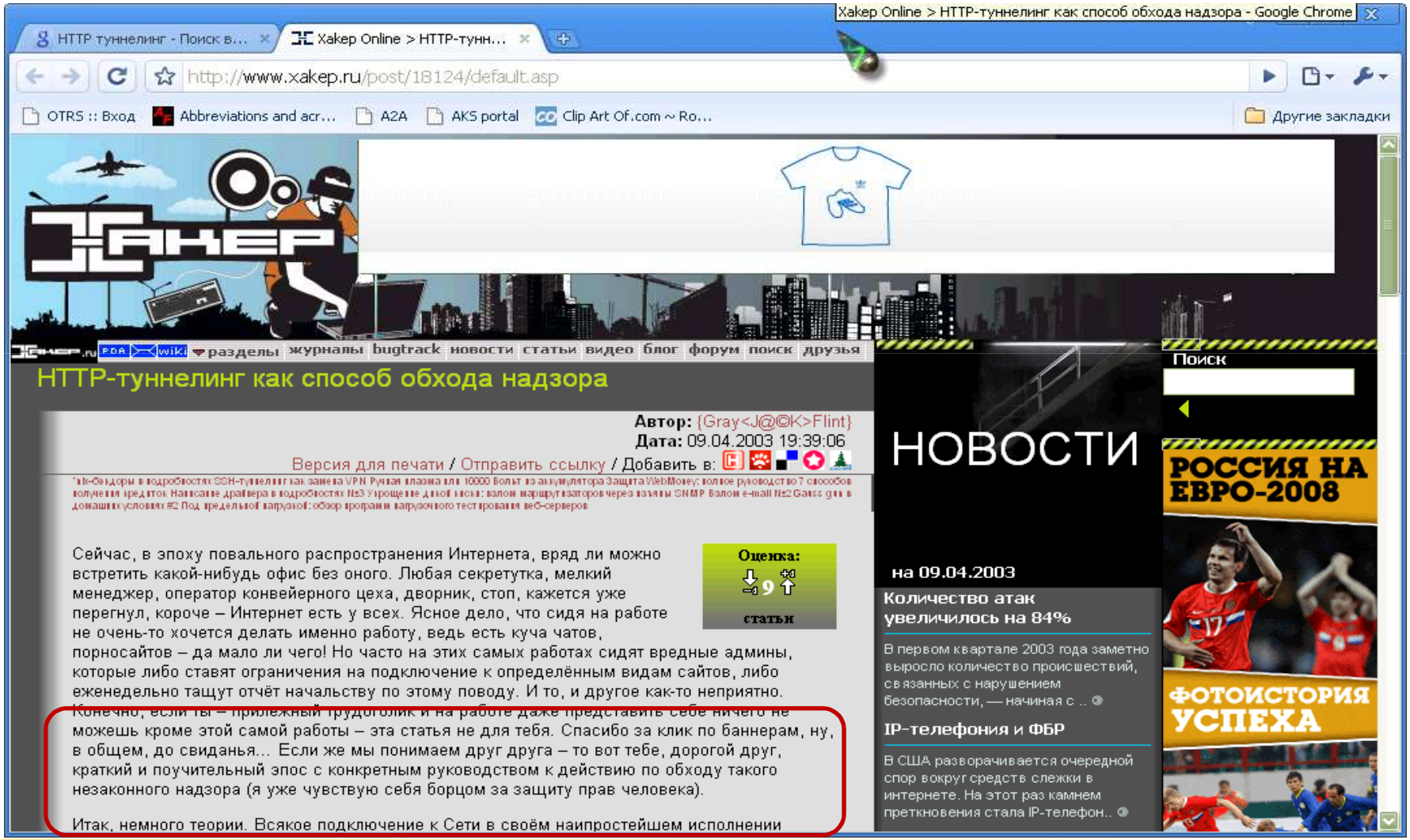
**Туннелинг**

- HAMACHI 4

**Трояны**

- SeeMe Backdoor 1
- Brontok.A 1

# Нелегитимные коммуникации



# Коммуникации шпионского ПО

**Spyware**

| | | |
|---|---|---|
| • QUADRO | | 38 |
| • EROR GUARD | 115 | |
| • ROGUE | | 112 |
| • EASYSEARCH (BI) | | 4 |
| • NEW.NET | | 13 |
| • GATOR | | 195 |
| • DIRECTWEBSEARCH | | 27 |
| • VISICOM (BI) | | 4 |
| • XXXTOOLBAR | 256 | |
| • DEBORAH | | 1 |
| • CMSINIT | | 1,392 |

# Файлообменные сети/IM

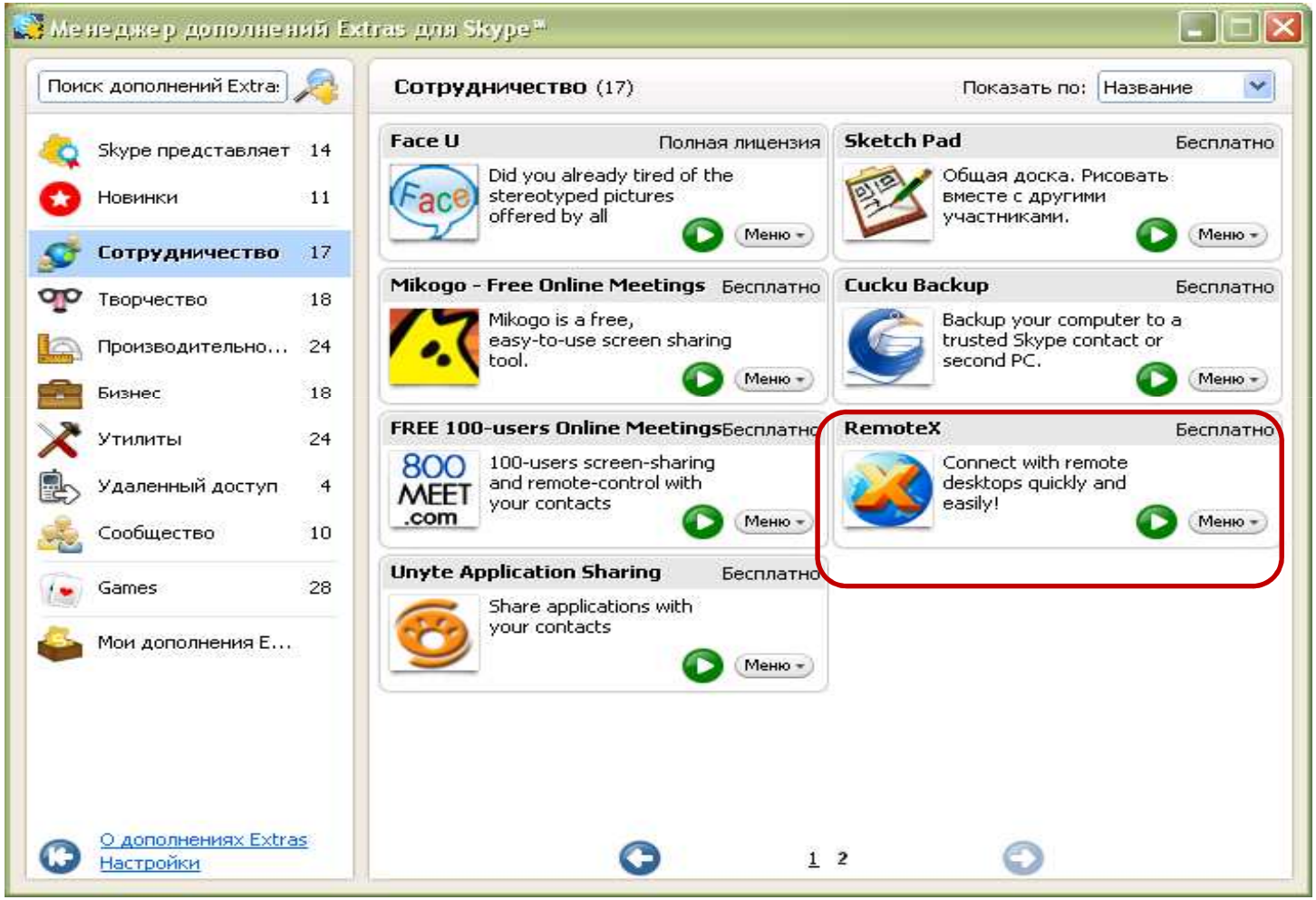
**Файлообменные сети (P2P)**

- GNUTELLA 5
- BITTORRENT 29,497
- DC++ 6
- EDONKEY 2000 13,995
- WAREZ 1
- WINMX 36
- SKYPE 530

**Передача файлов в IM**

- GOOGLE TALK 160
- ICQ/AOL 4

# Немного о Skype

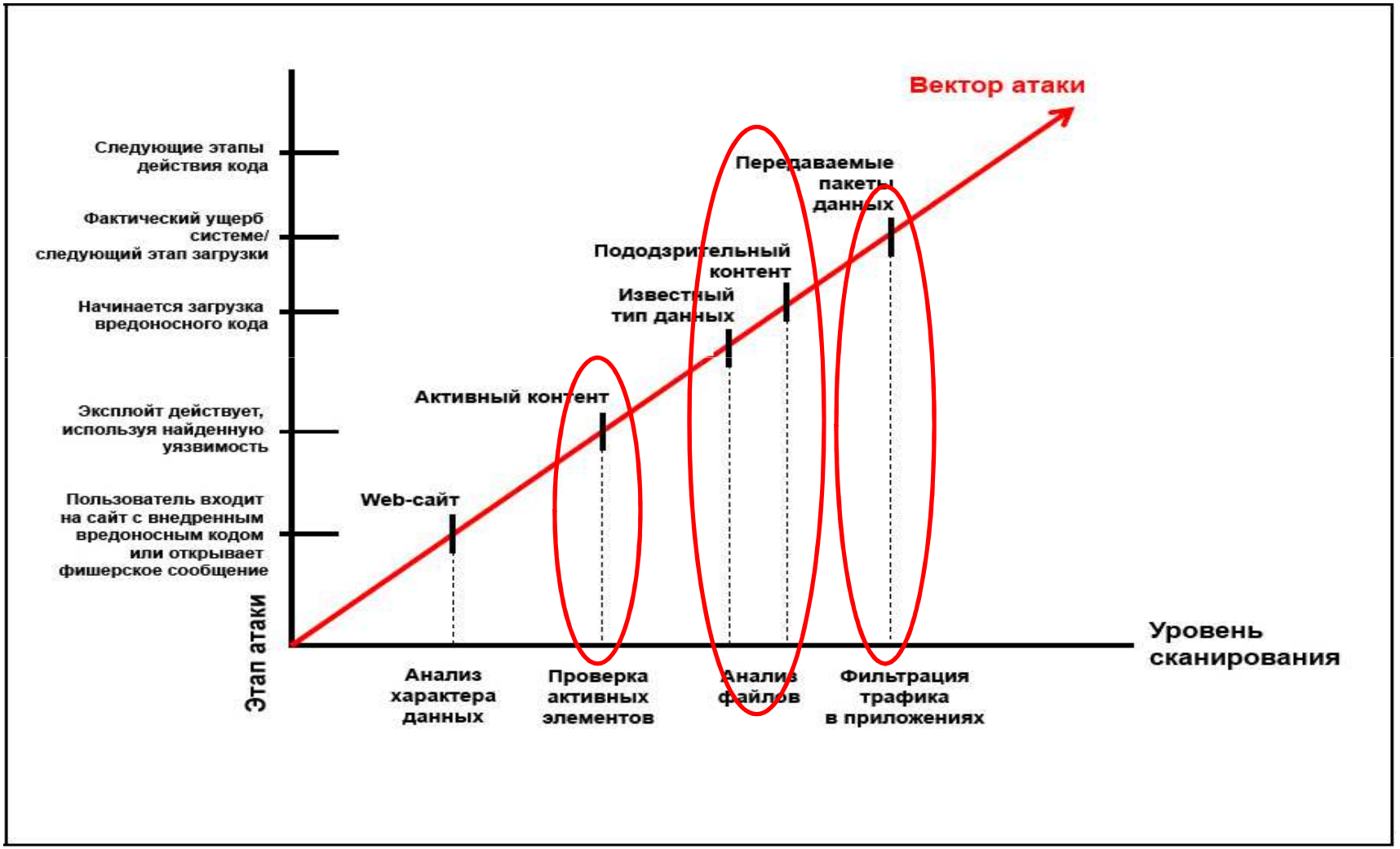


# Удаленное управление

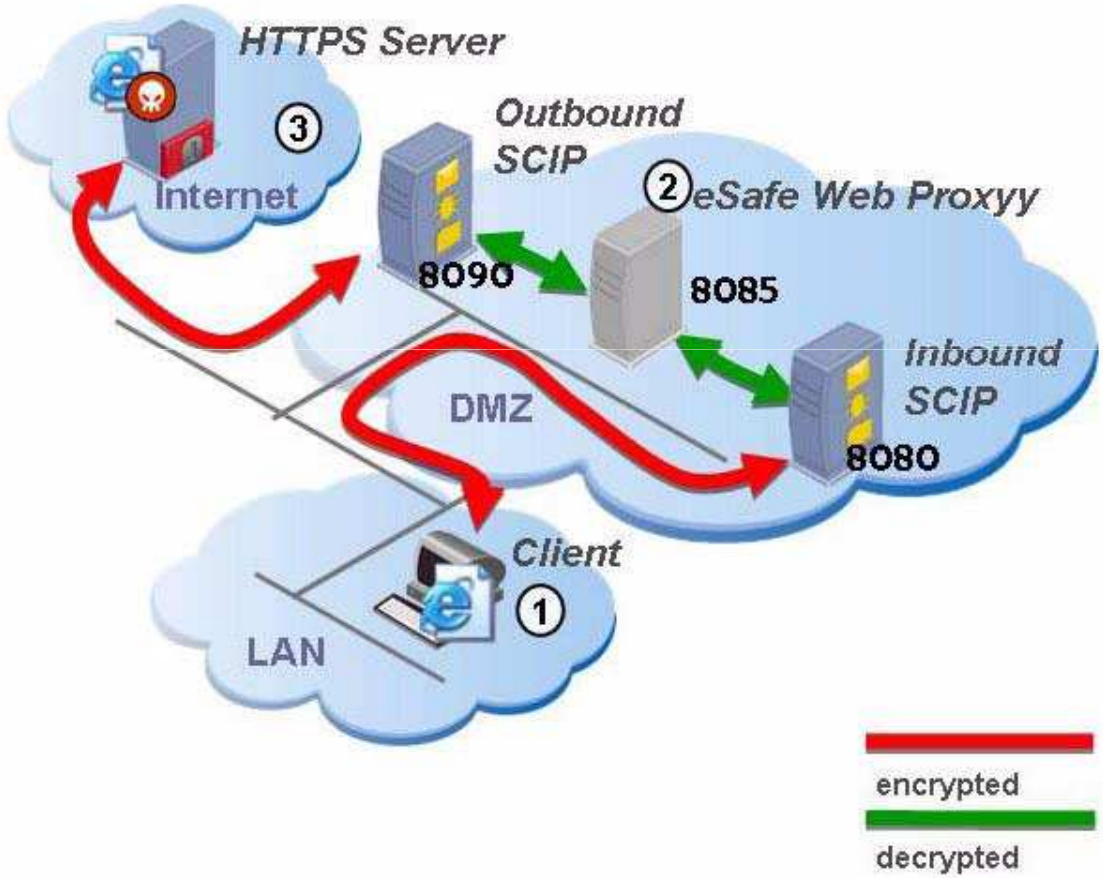
**REMOTE CONTROL**

- LOGMELN 4
- CITRIX 2
- RDP 5
- RADMIN 1

# Требования к защите



# Фильтрация SSL/TLS



# Выводы

DLP и CF – Противоречия нет. Важно правильно понимать возможности и верно расставлять приоритеты!


Как будет выглядеть трафик Вашей компании зависит только от Вас!

# БЛАГОДАРЮ ЗА ВНИМАНИЕ !

**ОРГАНИЗАТОРЫ**




Руководитель направления
контент-безопасности
Владимир Бычек

v.bychek@aladdin.ru