

Защита от угроз, передаваемых в шифрованном трафике

eSafe[®]

ОРГАНИЗАТОРЫ

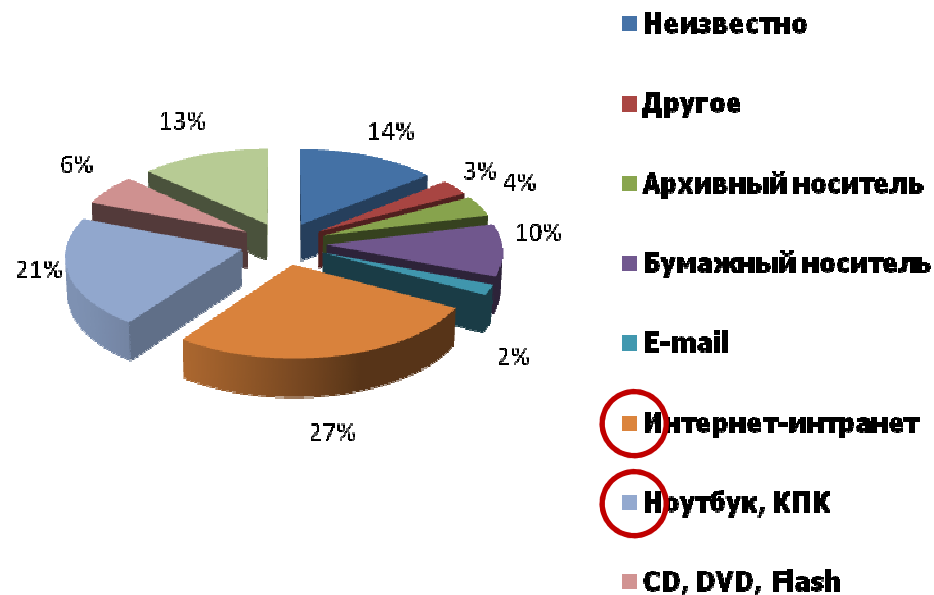
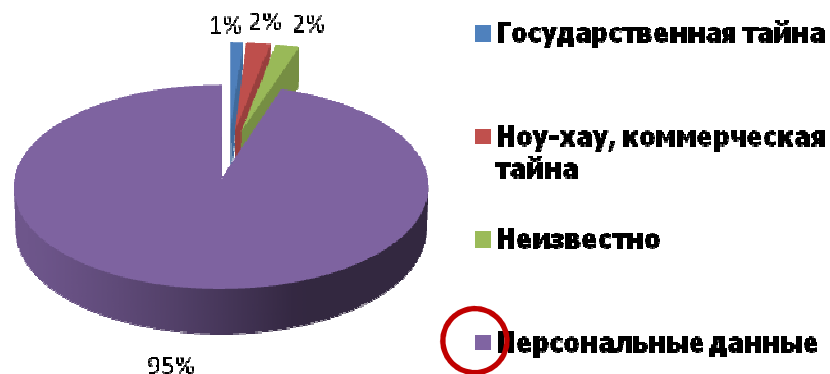


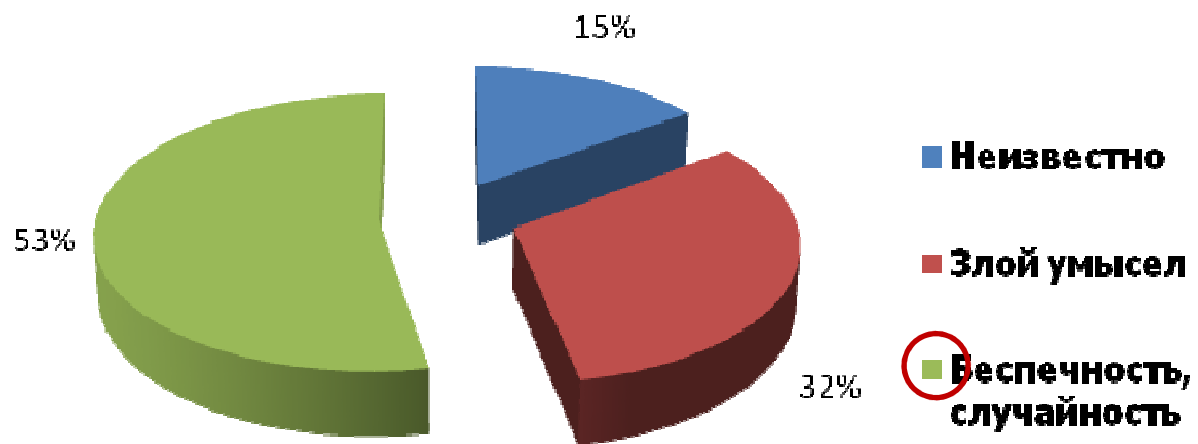
Руководитель направления
контент-безопасности
Владимир Бычек

v.byчек@aladdin.ru
5-6 ноября 2008

DLP vs. CF

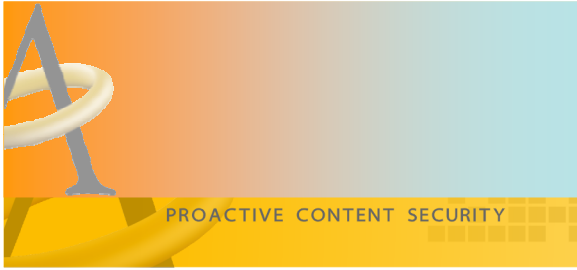






- Большая часть утечек происходит неумышленно. Перекрыть возможности случайной утечки означает решить проблему на три четверти. Борьба же с инсайдерами-злоумышленниками – это в среднем менее приоритетная и более сложная задача. При ограниченности средств её следует решать во вторую очередь.
- Мобильные 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.





PROACTIVE CONTENT SECURITY

СКРЫТЫЕ И НЕКОНТРОЛИРУЕМЫЕ КАНАЛЫ



eSafe[®] Схема включения

PROACTIVE CONTENT SECURITY



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



The screenshot shows a Google Chrome browser window with the address bar displaying `http://www.xakep.ru/post/18124/default.asp`. The page title is "HTTP-туннелинг как способ обхода надзора". The article text includes:

Автор: {Gray<J@>@K>Flint}
 Дата: 09.04.2003 19:39:06

Версия для печати / Отправить ссылку / Добавить в: [Social media icons]

Сейчас, в эпоху повального распространения Интернета, вряд ли можно встретить какой-нибудь офис без оного. Любая секретутка, мелкий менеджер, оператор конвейерного цеха, дворник, стоп, кажется уже перегнул, короче – Интернет есть у всех. Ясное дело, что сидя на работе не очень-то хочется делать именно работу, ведь есть куча чатов, порносайтов – да мало ли чего! Но часто на этих самых работах сидят вредные админы, которые либо ставят ограничения на подключение к определённым видам сайтов, либо еженедельно тащут отчёт начальству по этому поводу. И то, и другое как-то неприятно.

Конечно, если ты – прилежный трудолюбик и на работе даже представить себе ничего не можешь кроме этой самой работы – эта статья не для тебя. Спасибо за клик по баннерам, ну, в общем, до свиданья... Если же мы понимаем друг друга – то вот тебе, дорогой друг, краткий и поучительный эпос с конкретным руководством к действию по обходу такого незаконного надзора (я уже чувствую себя борцом за защиту прав человека).

Итак, немного теории. Всякое подключение к Сети в своём наипростейшем исполнении

Оценка: статьи

NOBOSTИ

на 09.04.2003

Количество атак увеличилось на 84%

В первом квартале 2003 года заметно выросло количество происшествий, связанных с нарушением безопасности, — начиная с...

IP-телефония и ФБР

В США разворачивается очередной спор вокруг средств слежки в интернете. На этот раз камнем преткновения стала IP-телефон...

РОССИЯ НА ЕВРО-2008

ФОТОИСТОРИЯ УСПЕХА

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 (P2P)

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

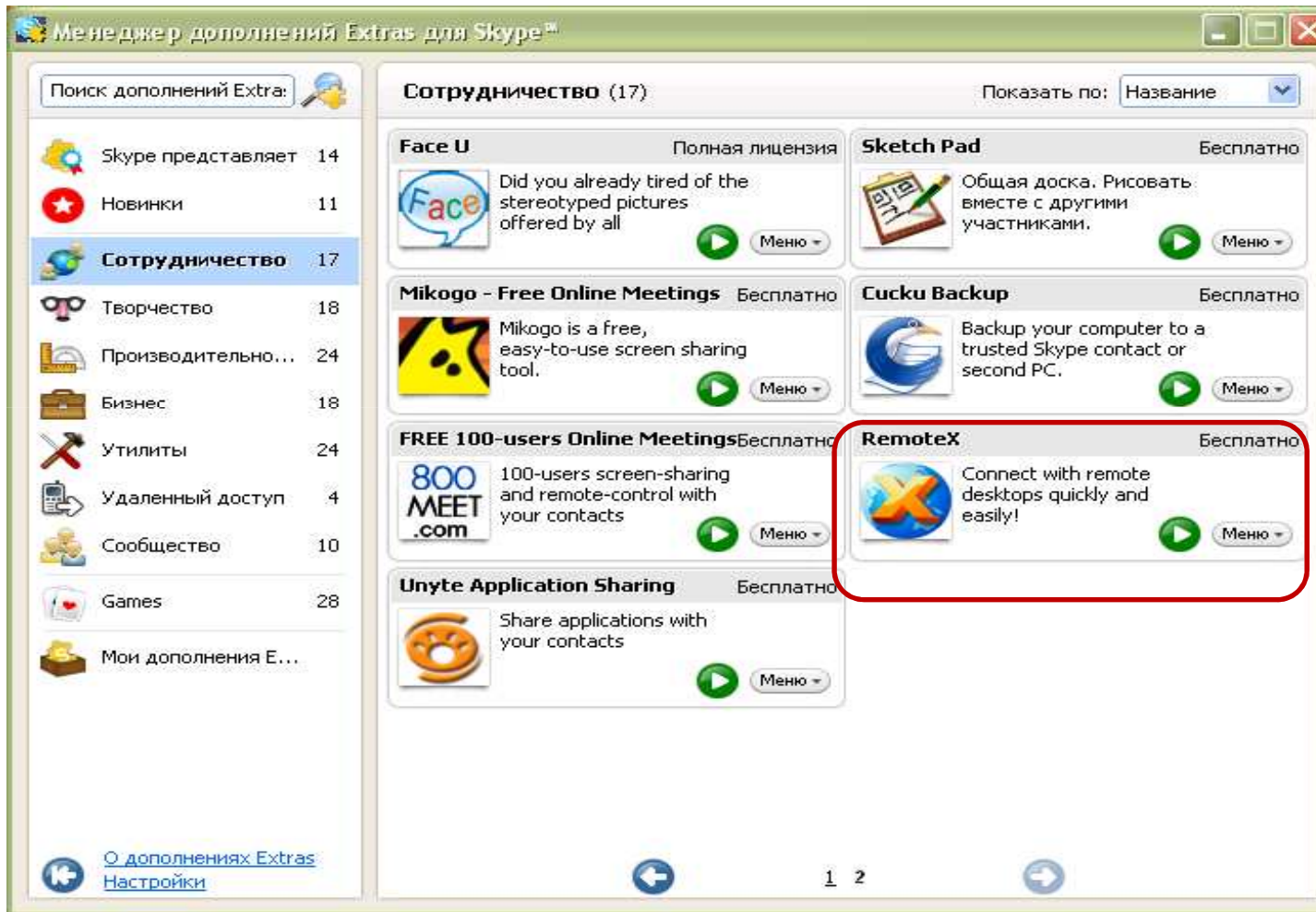
Передача файлов в IM

• GOOGLE TALK	160
• ICQ/AOL	4



eSafe[®] Немного о Skype

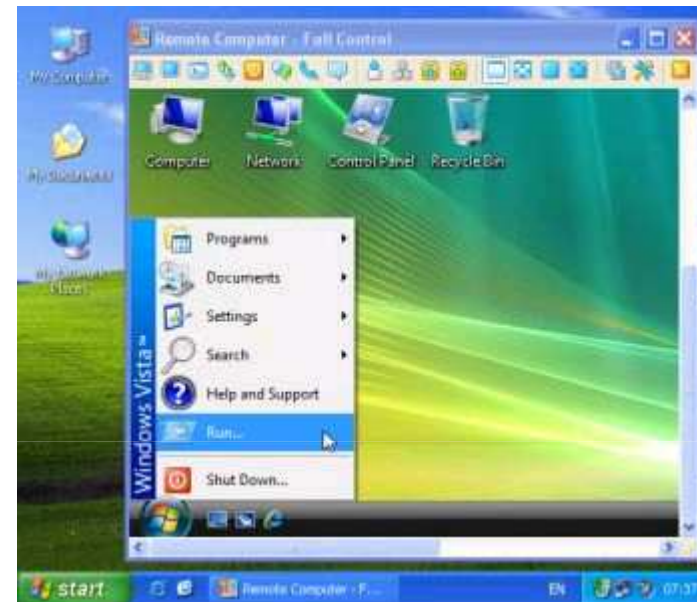
PROACTIVE CONTENT SECURITY



12

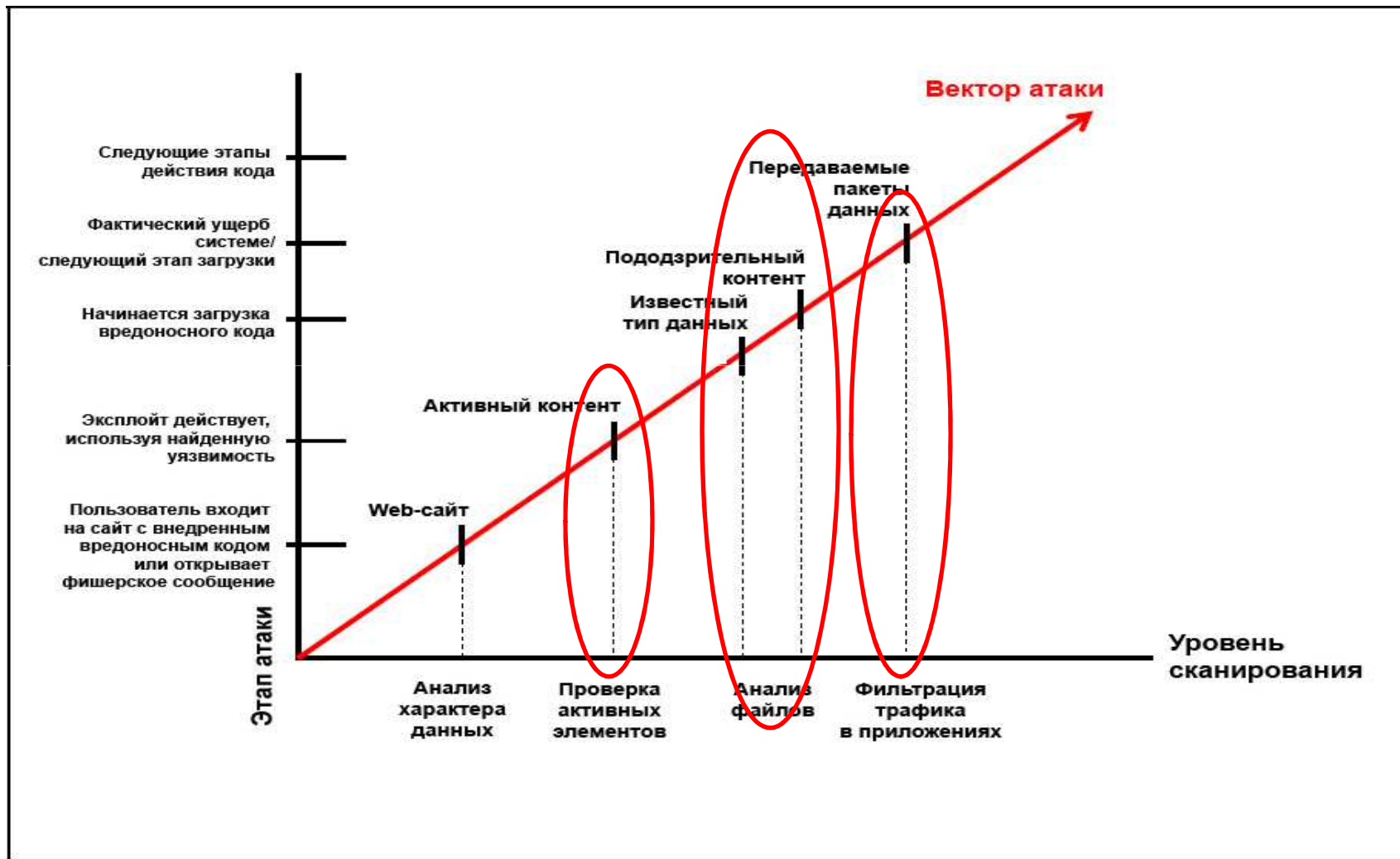
REMOTE CONTROL

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



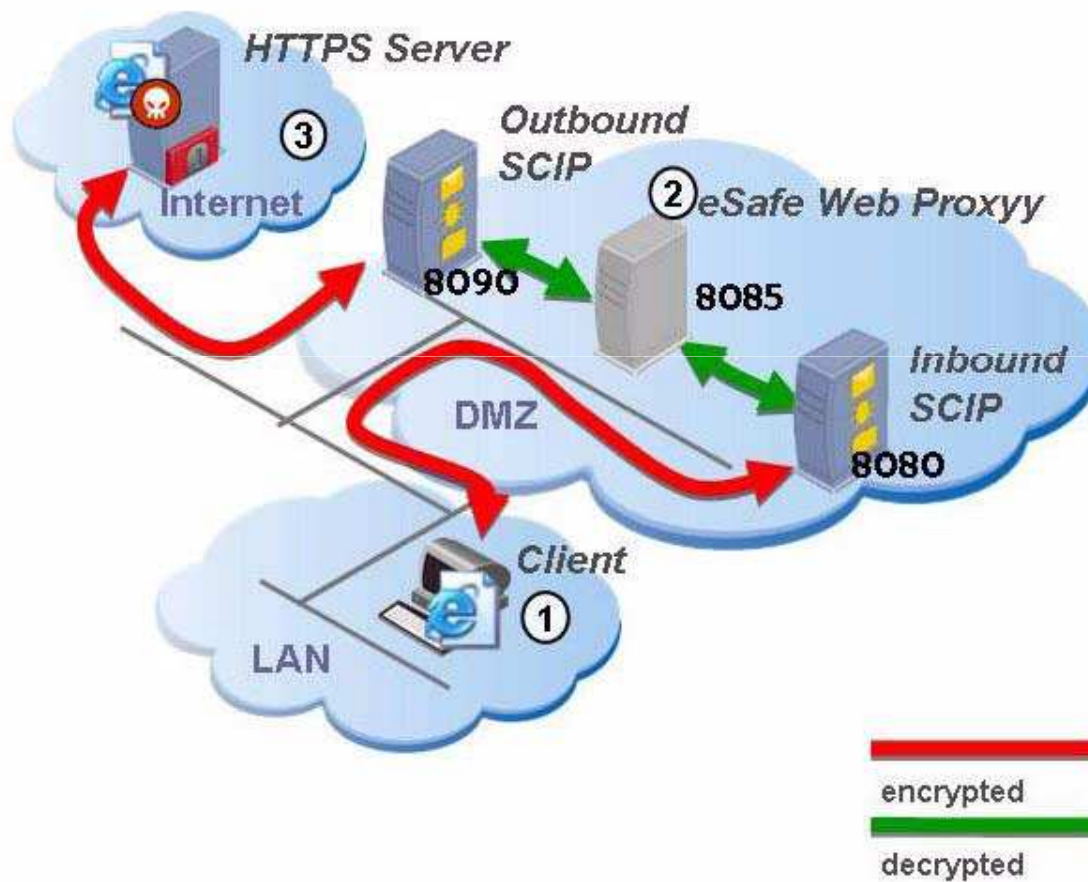
eSafe® Требования к защите

PROACTIVE CONTENT SECURITY



eSafe® Фильтрация SSL/TLS

PROACTIVE CONTENT SECURITY



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.byчек@aladdin.ru

17