

# DLP-системы – современные средства борьбы с инсайдерами

Илья Шабанов  
Управляющий партнер

- Что такое DLP с точки зрения аналитика?
- Рынок средств защиты от утечки конфиденциальных данных в России
  - Состояние рынка
  - Объем рынка и основные игроки
- Тенденции на рынке
  - Технологические тенденции
  - Эволюция применимости
  - Интеграция со сторонними решениями
- Новые вызовы

Средство защиты	Применение	Минусы
Классические антивирусы и сетевые экраны	Возможное обнаружение атаки	Бесполезны против целевых атак или действий инсайдеров
Шифрование	Защита от случайных утечек	Бесполезны против умышленных утечек
DLP-решения, включая близкие к ним (например, контроль портов)	Обнаружение несанкционированных действий с конфиденциальными данными	Недостаточно эффективны против умышленных утечек, могут быть сложны во внедрении
Rights Management Services (RMS)	Защита от случайных утечек	Бесполезны против умышленных утечек, сложны во внедрении и использовании

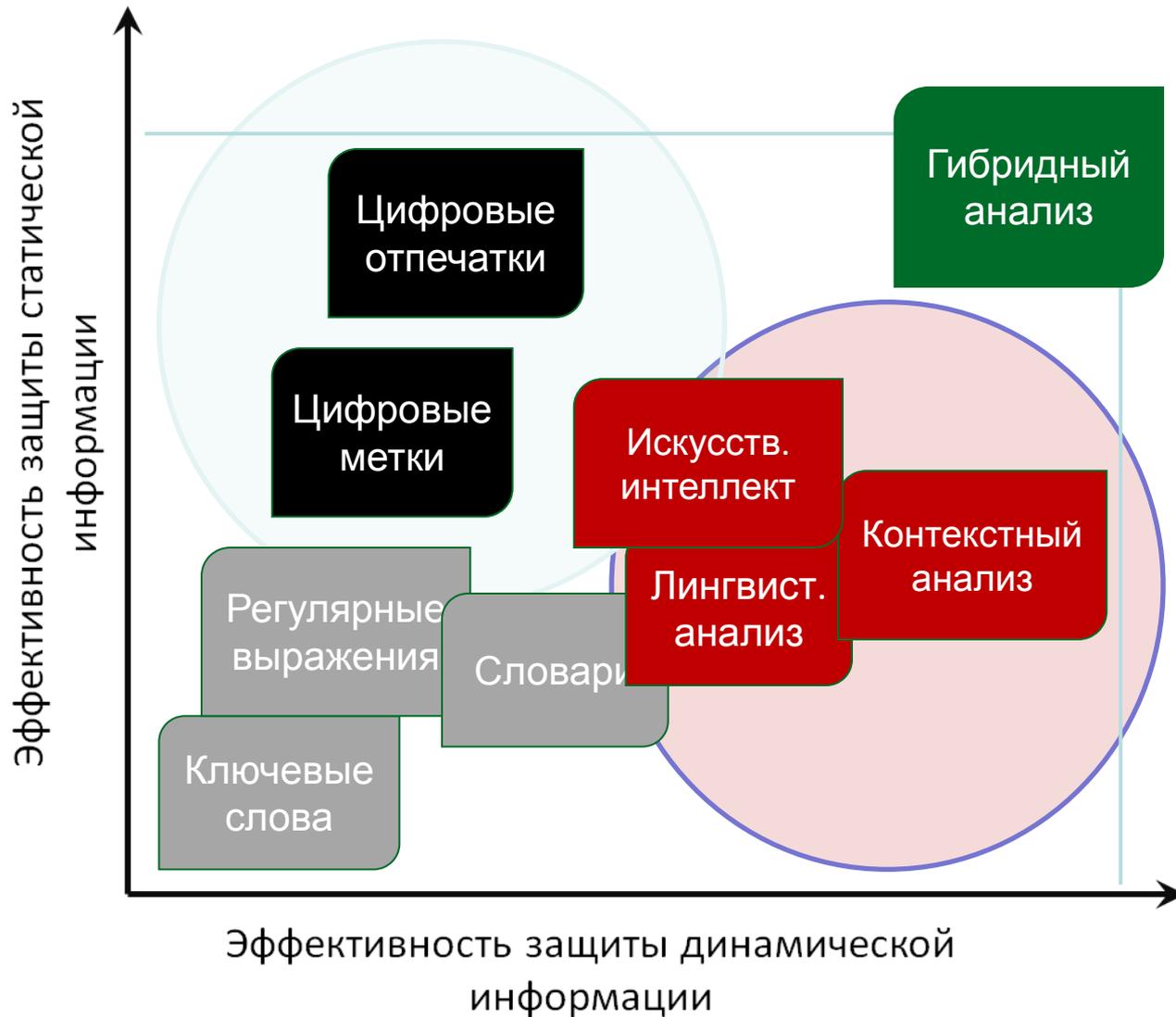
DLP-продукт обнаруживает и/или блокирует несанкционированную передачу конфиденциальной информации (утечку) по каналам:

- Электронная почта (трафик SMTP, POP3, IMAP)
- Веб-ресурсы (трафик HTTP, HTTPS и FTP)
- ICQ, Jabber, MSN, Skype, P2P-клиенты
- Сетевая печать
- Передача на внешние устройства

## Атрибуты современной DLP-системы:

- Создание политик контроля данных
- Анализ контента и действий с ним (создание, копирование, изменение, передача и т.д.)
- Анализ контекста действий с данными (кем, кому и как передаются данные)
- Возможности блокирования утечки
- Оповещение о произошедшей или успешно заблокированной утечке
- Архив событий и инструменты пост-анализа для расследований

Технология	Особенности и преимущества
Словари и регулярные выражений	Позволяет обнаруживать утечки данных, содержащих наборы слов или цифр
Лингвистический и контекстный анализ	<b>Проактивная</b> защита только конфиденциальных данных, сразу после их создания
Цифровые отпечатки или метки	Защита <b>редко изменяемых</b> конфиденциальных данных, которые были предварительно найдены и проиндексированы
Искусственный интеллект	Самообучающиеся алгоритмы детектирования

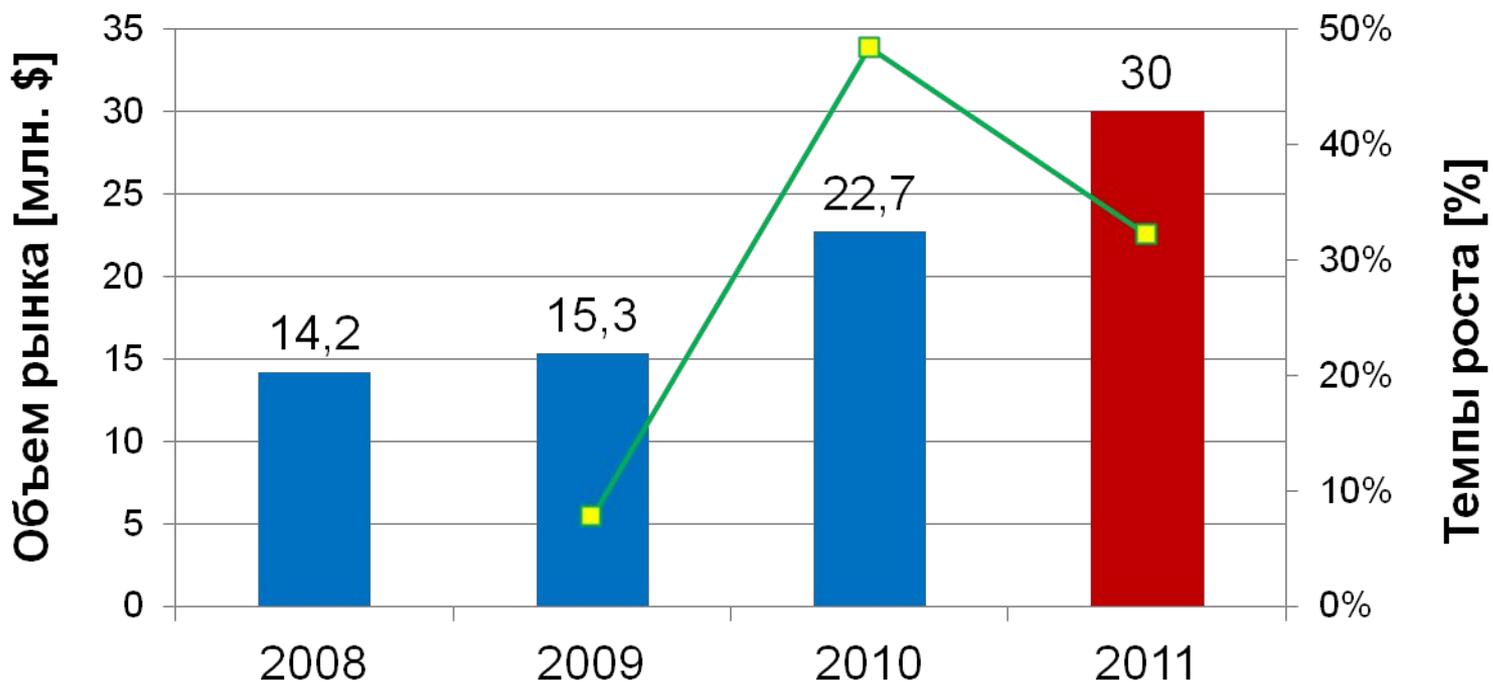


Эффективность гибридного анализа выше благодаря слиянию наиболее эффективных технологий

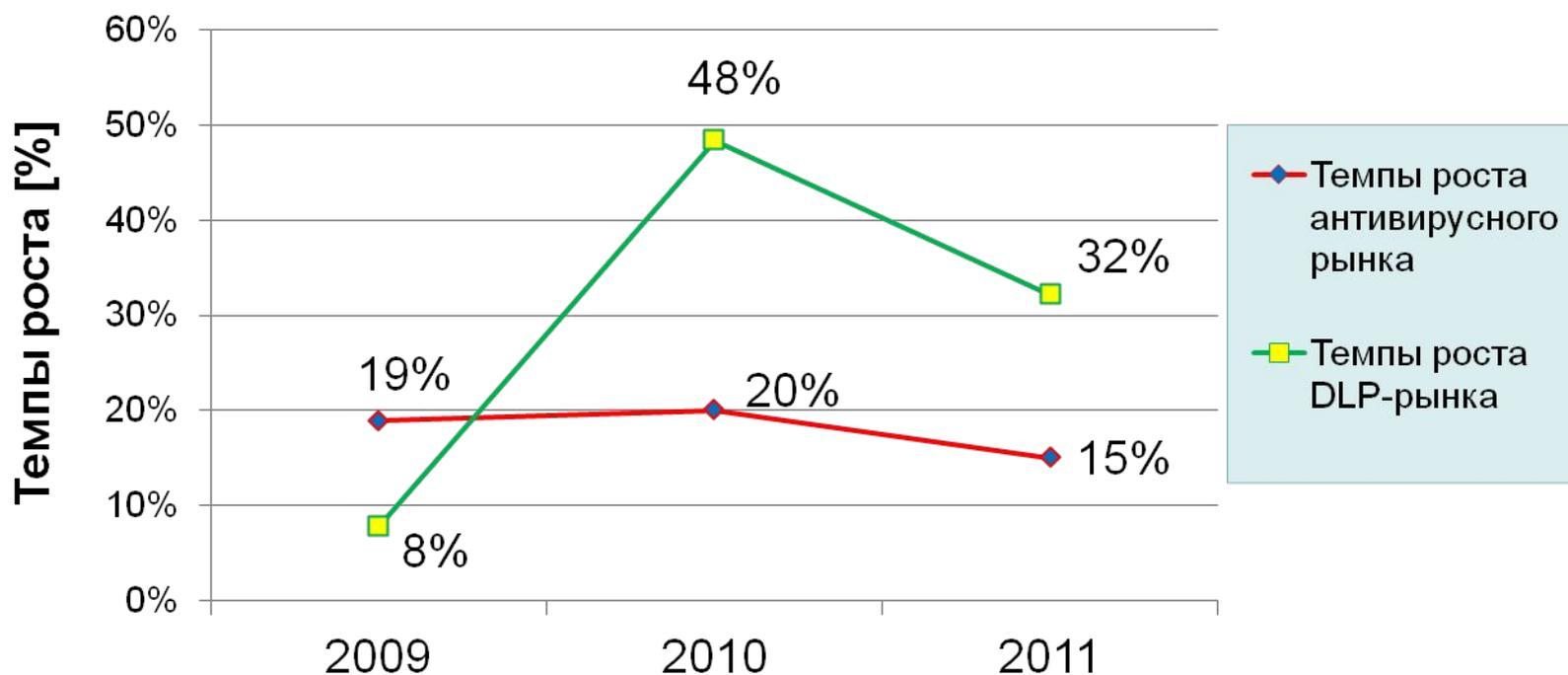


Какой DLP покупают в России?

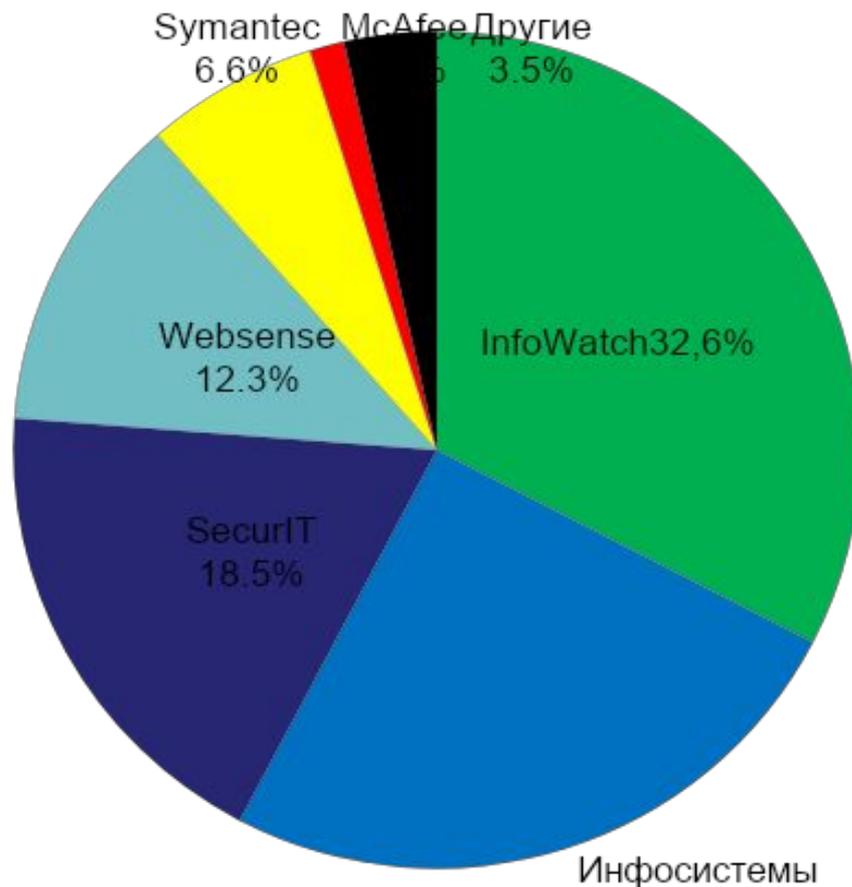
Объем DLP-рынка в России в 2008-2010 годах (млн. USD)



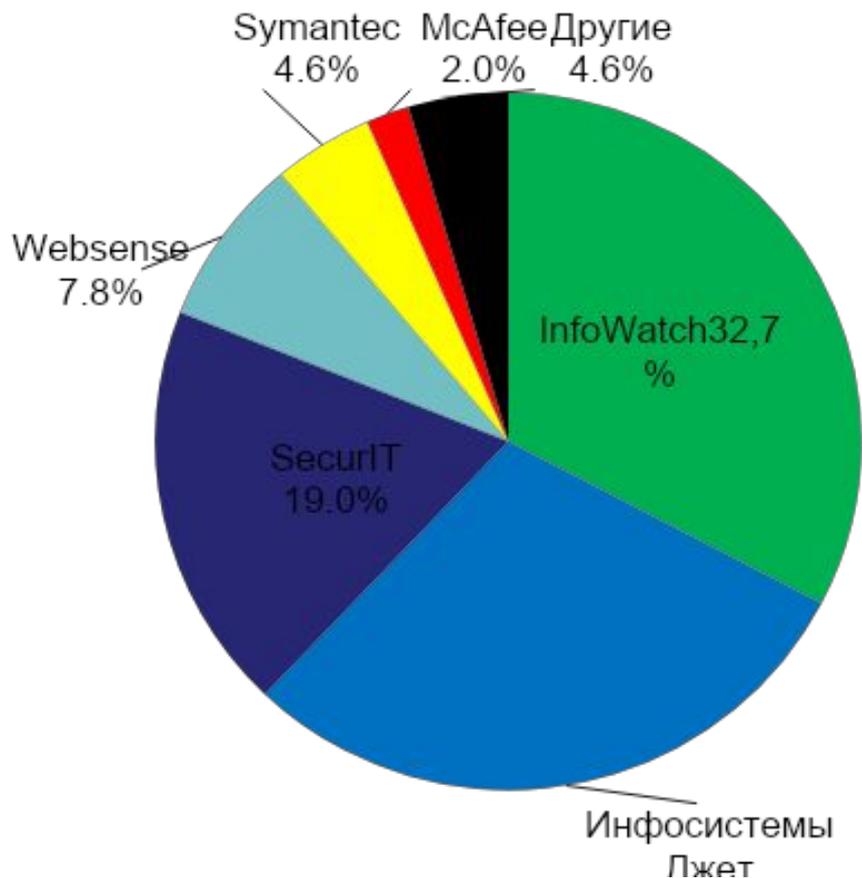
Объем DLP-рынка в России в 2008-2010 годах (млн. USD)



## Доли рынка участников DLP-рынка в России в 2010 году

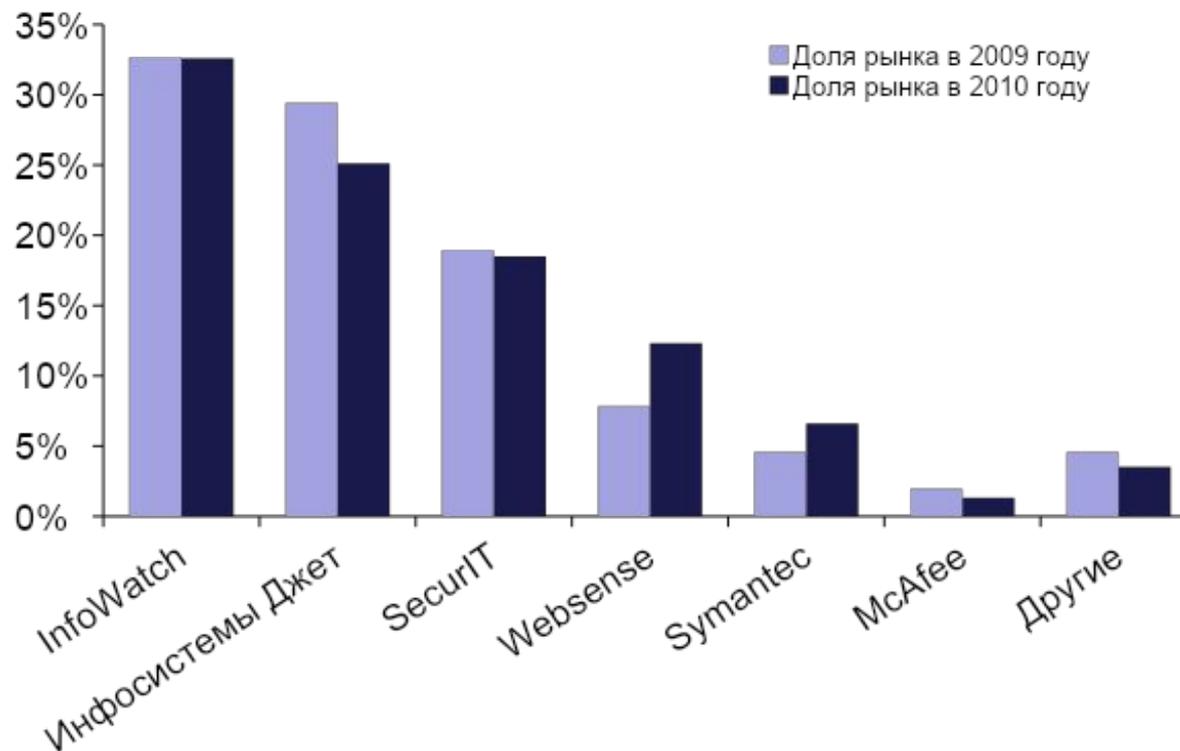


## Доли рынка участников DLP-рынка в России в 2009 году

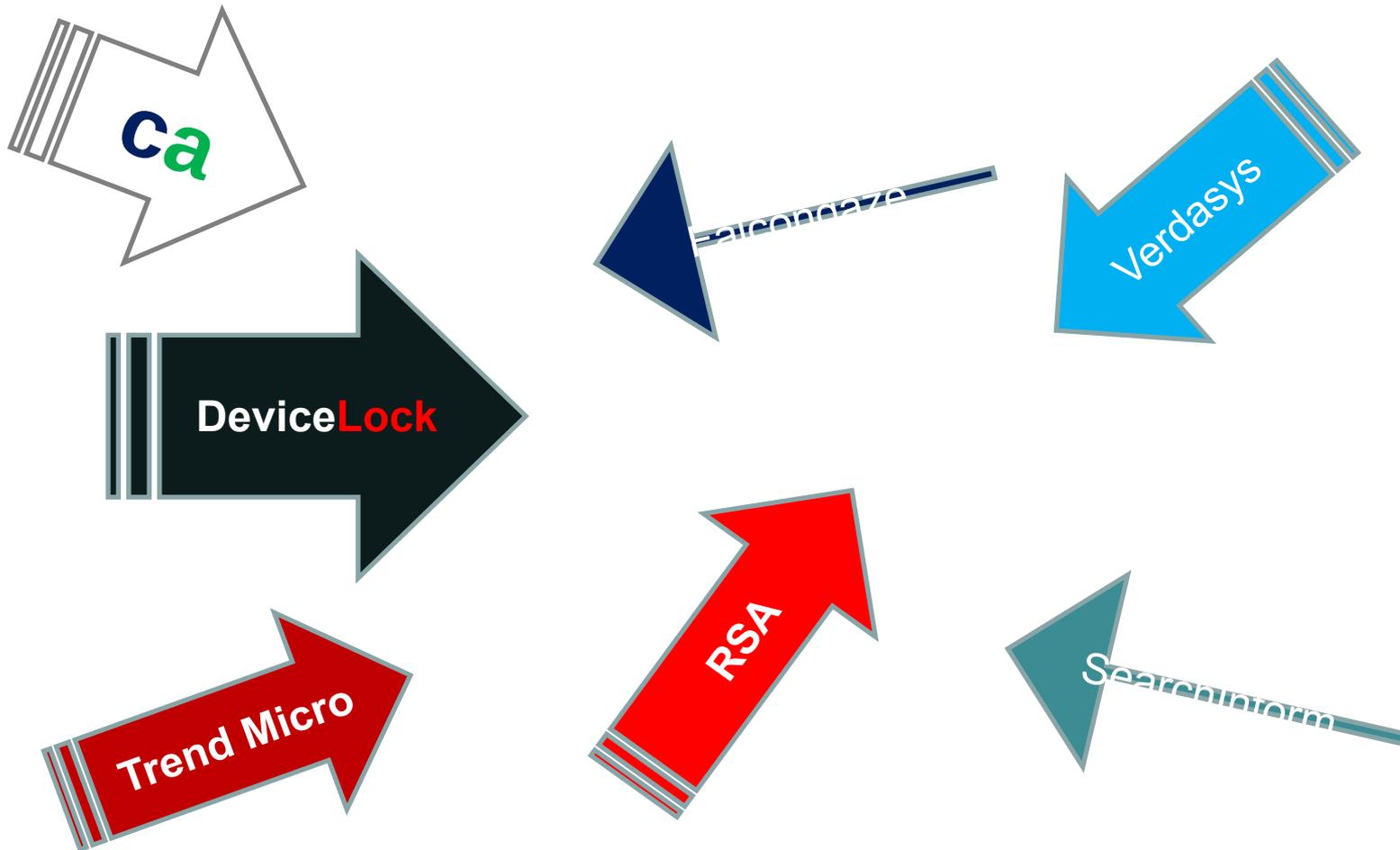


Производитель	Доля рынка 2009	Доля рынка 2010	Изм. доли рынка 2009-2010
InfoWatch	32,7%	32,6%	-0,1%
Инфосистемы Джет	29,4%	25,1%	-4,3%
SecurIT	19,0%	18,5%	-0,5 %
Websense	7,8%	12,3%	4,5%
Symantec	4,6%	6,6%	2,0%
McAfee	2,0%	1,3%	- 0,6%
Другие	4,6%	3,5%	-1,1%

## Изменение долей DLP-рынка в России в 2010 году



Конкуренция на рынке постоянно возрастает



- Объем российского рынка DLP пока остается небольшим и он постепенно «размывается».
- Уровень конкуренции на рынке растет быстрее, чем его объем.
- Тема утечек из российских компаний остается крайне закрытой. Внутренним угрозам не уделяется большего внимания.
- Против рынка работает привитый за годы некоторыми вендорами стереотип о сложности и дороговизне защиты от утечек.

Для выхода на массового потребителя нужны другие решения – проще, дешевле, удобнее.



Что ожидать в ближайшем будущем?

- Рост функциональности и зрелости продуктов
  - Контроль большего количества каналов
  - Совершенствование систем анализа событий
  - Упрощение внедрения и настройки
- Совершенствование технологий детектирования
  - Гибридные технологии
  - Самообучающиеся статистические технологии
- Автоматизация начальной настройки и обучения системы

Массовый потребитель ждет простого и эффективного решения по адекватной цене

- Предотвращение нежелательных или криминальных действий сотрудников
- Контроль настроек внутри компании
- Контроль действий сотрудников на рабочем месте
- Расследование инцидентов

Функции современных DLP-решений выходят далеко за рамки первоначального определения этого рынка

Интеграция со сторонними решениями:

- Системы шифрования данных
- Rights Management Services (RMS)
- Заимствование функций систем контроля деятельность персонала
- Интеграция функцией в состав комплексных шлюзовых продуктов (UTM)

Как отвечать на глобальные вызовы IT-рынка?

- Контроль мобильных устройств
- Виртуализация и «облака»
- Утечки связанные не использованием вредоносных программ
- Сквозные политики безопасности, автоматическое принятие решений (логические триггеры)

DLP-рынок пока не предлагает решений этих проблем, делаются только первые шаги

Спасибо за внимание!

Вопросы?

**Илья Шабанов**

[Ilya.shabanov@anti-malware.ru](mailto:Ilya.shabanov@anti-malware.ru)

<http://www.anti-malware.ru>