Data *Luxury* Protection (DLP) – защита данных *с удовольствием!*

Валерий Боронин

руководитель лаборатории защиты информации от внутренних угроз,
Лаборатория Касперского

DLP Research, R&D, Kaspersky Lab

28 октября 2011

InfoProstranstvo, Moscow

IV международная конференция

DLP-Russia

Protect your inner space

Разрешите представиться!
Об авторе

Валерий Боронин,
руководитель лаборатории защиты информации от внутренних угроз, ЗАО "Лаборатория Касперского".

- В индустрии **15+** лет, в «безопасности» с **1999**
- В ЛК отвечаю за исследования и разработку **технологий** в области **DLP** и защиты данных

- До ЛК трудился в
  - Entensys (продукты семейства UserGate, CTO)
  - Lumension (линейка Application & Device Control)
  - TrustDigital (стартап поглощен McAfee в 2010)
  - Parallels (бывший SwSoft) и других
- Консультировал и работал на заказ

Кто это?

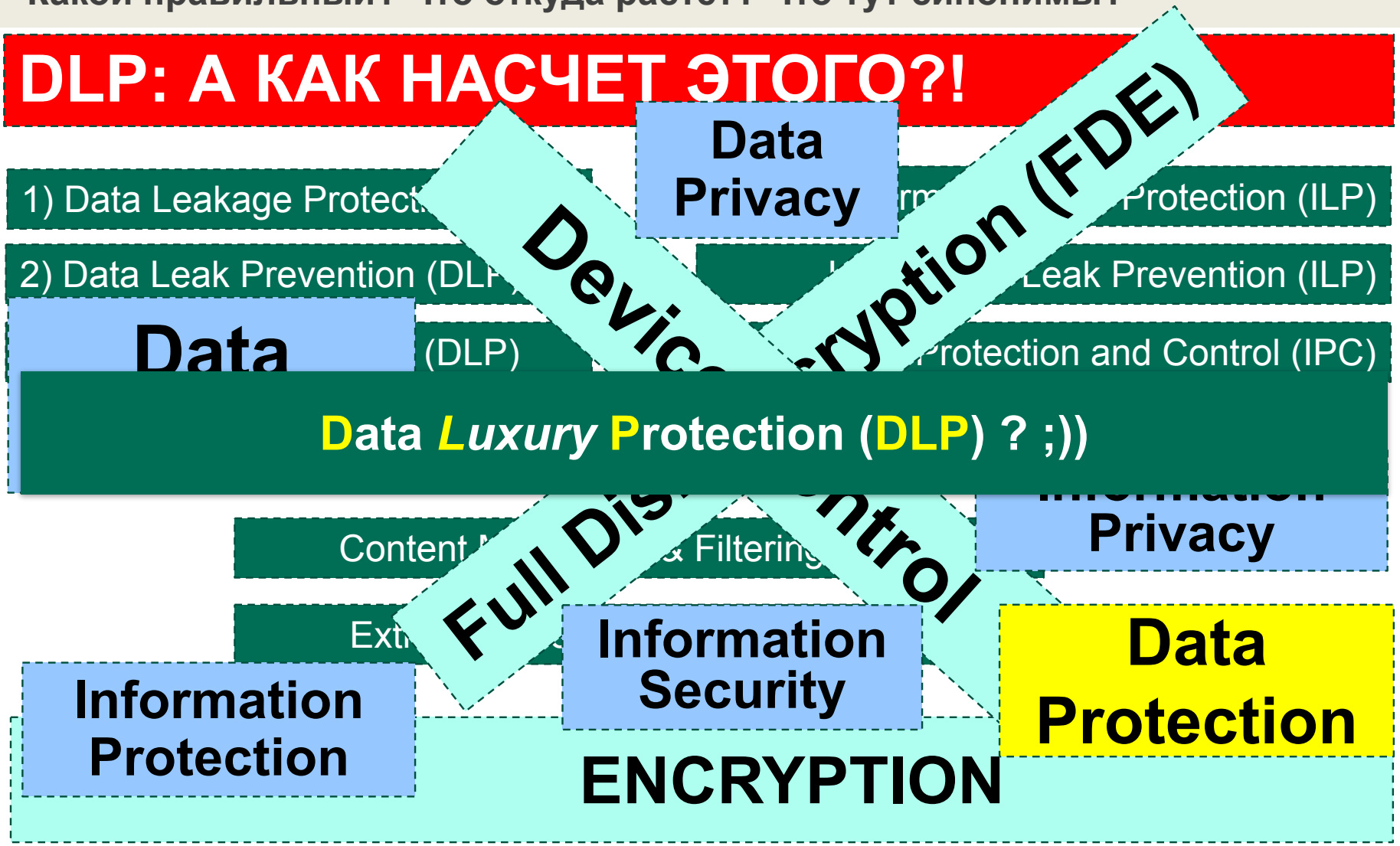
И как эти люди связаны с темой?

Data
***L*uxury**
Protection

KASPERSKY lab

Защита данных. DLP. Мириады определений и терминов

Какой правильный? Что откуда растет? Что тут синонимы?



Data Privacy: 4 Требования и 7 Принципов

Всесторонняя, хорошо продуманная программа защиты данных учитывает:

Confidentiality — the need to protect against unauthorized access to information

Integrity — the ability to ensure that information is not improperly changed/deleted

Availability — the ability to provide appropriate access to stakeholders

Privacy — the assurance that personal information is used only for the specific business purpose for which it was collected

The 7 principles governing the OECD's recommendations for protection of personal data

Notice *- data subjects should be given notice when their data is being collected;*

Purpose *- data should only be used for the purpose stated and not for any other purposes;*

Consent *- data should not be disclosed without the data subject's consent;*

Security *- collected data should be kept secure from any potential abuses;*

Disclosure *- data subjects should be informed as to who is collecting their data;*

Access *- data subjects should be allowed to access their data and make corrections to any inaccurate data;*

Accountability *- data subjects should have a method available to them to hold data collectors accountable for following the above principles.*[2]

Откуда начинается защита данных? Privacy.

Privacy (Права Человека и Закон)

Data Privacy (Люди и Процессы, ПО и Железо)

Information (данные, имеющие смысл**) Privacy**

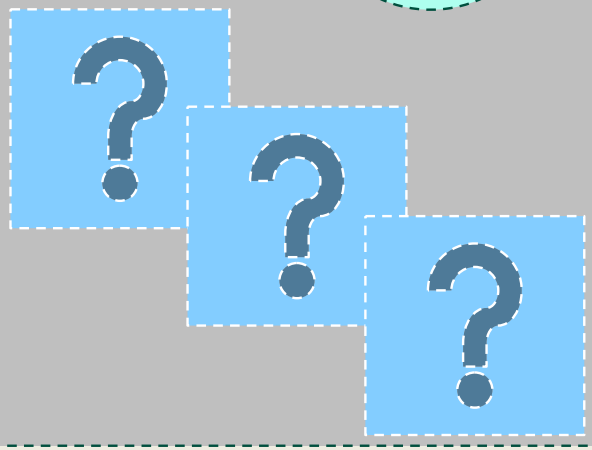
Data Security = Data Protection

Information Security = Information Protection

DLP – Data Loss Prevention

- **Data Leakage Protection (DLP)**
- **Information Leak Protection (ILP)**
- **Information Leak Prevention (ILP)**
- **Information Protection and Control (IPC)**
- **Information Leak Detection & Prevention (ILDP)**
- **Content Monitoring and Filtering (CMF)**
- **Extrusion Prevention System (EPS)**

Технологии защиты данных включают в себя широкий набор решений предназначенных для защиты конфиденциальных данных при их **хранении, передаче или использовании**



Information Protection

Identify **Who, What, Where and When** of data access. **Availability.**

IAM

Confidentiality & Integrity
Risks Data Loss & Theft

Encryption

Deep Content Inspection + **Context Rules**

Content-Aware DLP

Disclosure. Audit. Restrict distribution and use of assets

E-DRM/RMS

What should be **monitored** and **where**. **Ex: SIEM, DAM**

Monitoring

ПЕРЕХОД ОТ DLP - К DATA PROTECTION

Security Controls are Preventive and Detective

Data Protection

Identify **Who, What, Where and When** of data access. **Availability.**

IAM

Confidentiality & Integrity
Risks Data Loss & Theft

Encryption

Deep Content Inspection + Context Rules

Content-Aware DLP

Disclosure. Audit. Restrict distribution and use of assets

E-DRM/RMS

What should be monitored and where. Ex: SIEM, DAM

Monitoring

КАКОЙ МЫ ВИДИМ ЗАЩИТУ ДАННЫХ СЕЙЧАС?

Иногда мы слышим о DLP…

МНЕНИЯ И ОТЗЫВЫ

СЛОЖНЫЕ

ТЯЖЁЛЫЕ

НЕУДОБНЫЕ

КОРЯВЫЕ

НЕНАДЁЖНЫЕ

НЕПОНЯТНЫЕ

НЕПРЕДСКАЗУЕМЫЕ

БЕСПОЛЕЗНЫЕ

ДОРОГИЕ

СЛОЖНЫЕ

ЭМОЦИИ И ОЩУЩЕНИЯ

БЕСПОКОЙСТВО
И НЕУВЕРЕННОСТЬ

НЕДОВЕРИЕ
и СОМНЕНИЕ

СОЖАЛЕНИЕ

ТЩЕТНОСТЬ И
БЕССМЫСЛЕННОСТЬ

РАЗОЧАРОВАНИЕ

ПЕССИМИЗМ

НЕВЕРИЕ

НЕПРИЯТИЕ

DLP СЕГОДНЯ – ЧТО НУЖНО УЛУЧШАТЬ?
И ГДЕ НАМ ВЗЯТЬ УДОВОЛЬСТВИЕ?!

DLP БУДУЩЕГО - РЕЗЕРВЫ ДЛЯ РОСТА:

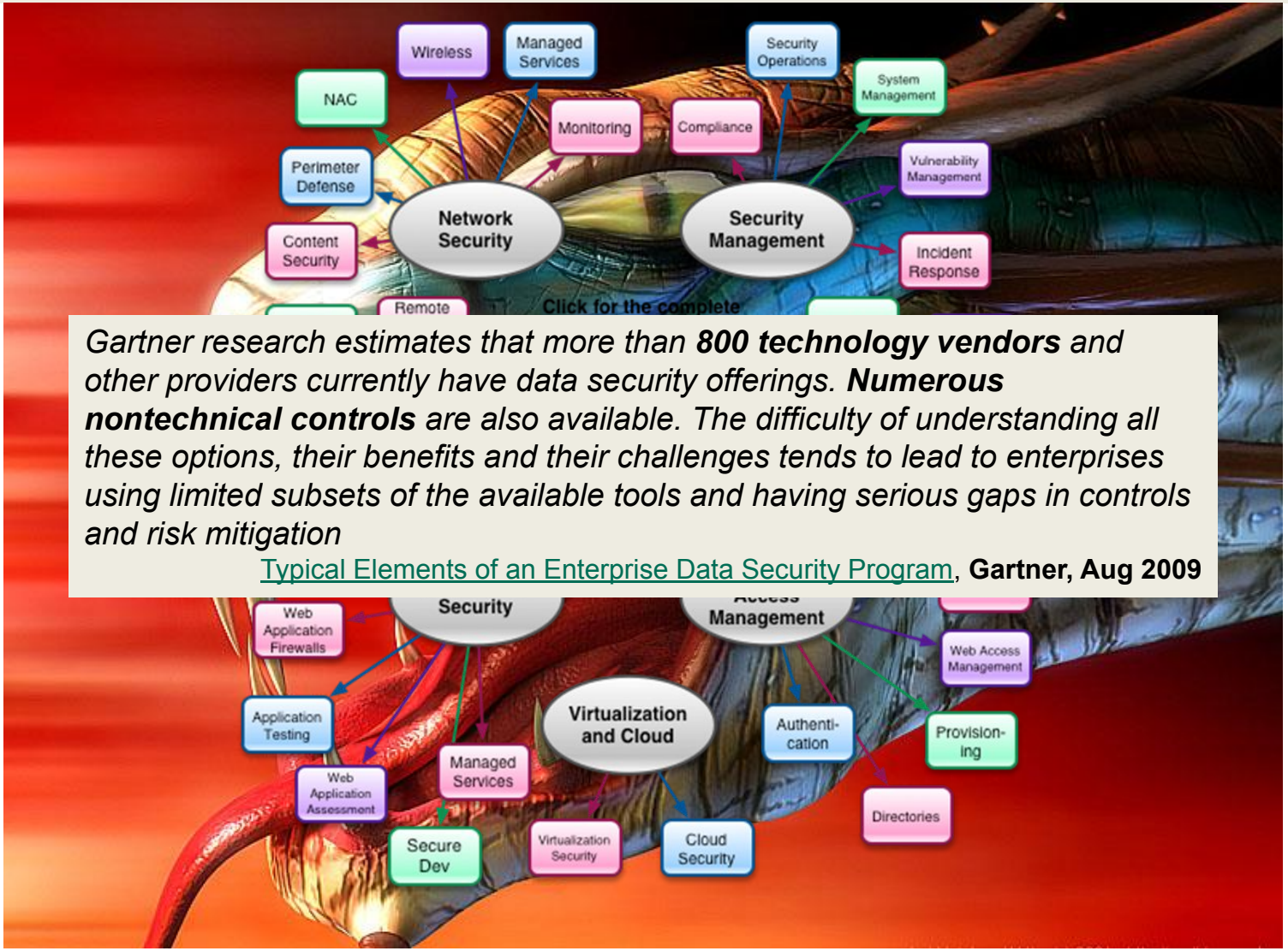
1. **СЛОЖНОСТЬ –> НЕНАДЕЖНОСТЬ –> НЕУДОБСТВО –> НЕЭФФЕКТИВНОСТЬ –> ДОРОГО**
2. **ЧЕЛОВЕЧЕСКИЙ ФАКТОР** учитывается недостаточно **РЕГЛАМЕНТЫ** отсутствуют или не слишком работают

DLP на практике: доказать нарушение легко, а вот умысел и *причастность* человека очень сложно, т.к.
«Логи ведут к Компьютеру, а не к Человеку»

3. **АВТОМАТИЗАЦИЯ** в зачаточном состоянии
4. **НЕТ ОТКРЫТЫХ СТАНДАРТОВ** – «привязка» к ПО
5. **НЕТ ОБЪЕДИНЯЮЩЕГО ИНСТРУМЕНТАРИЯ**

1. DLP СИСТЕМЫ СЕГОДНЯ - В ЧЕМ СЛОЖНОСТЬ?

1000 ТЕХНОЛОГИЙ!



*Gartner research estimates that more than **800 technology vendors** and other providers currently have data security offerings. **Numerous nontechnical controls** are also available. The difficulty of understanding all these options, their benefits and their challenges tends to lead to enterprises using limited subsets of the available tools and having serious gaps in controls and risk mitigation*

Typical Elements of an Enterprise Data Security Program, **Gartner, Aug 2009**

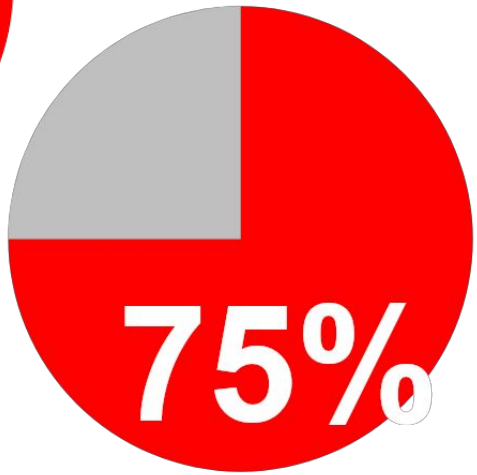
2. ЛЮДИ. ЧЕЛОВЕЧЕСКИЙ ФАКТОР учитывается слабо

Зачем нужна осведомлённость (User Awareness)

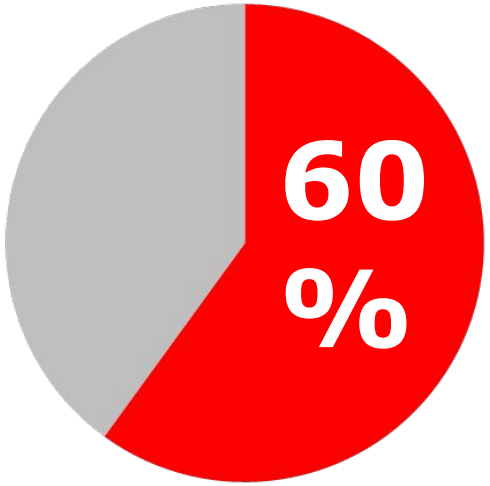
Человек – самое слабое звено.
Что делать? (кликабельно)
ЗАЩИТИТЬ!

успешных APT атак направлены на человека (Mandiant)

Зловредов нужно участие пользователя (Symantec)



инцидентов из-за «человеческого фактора»

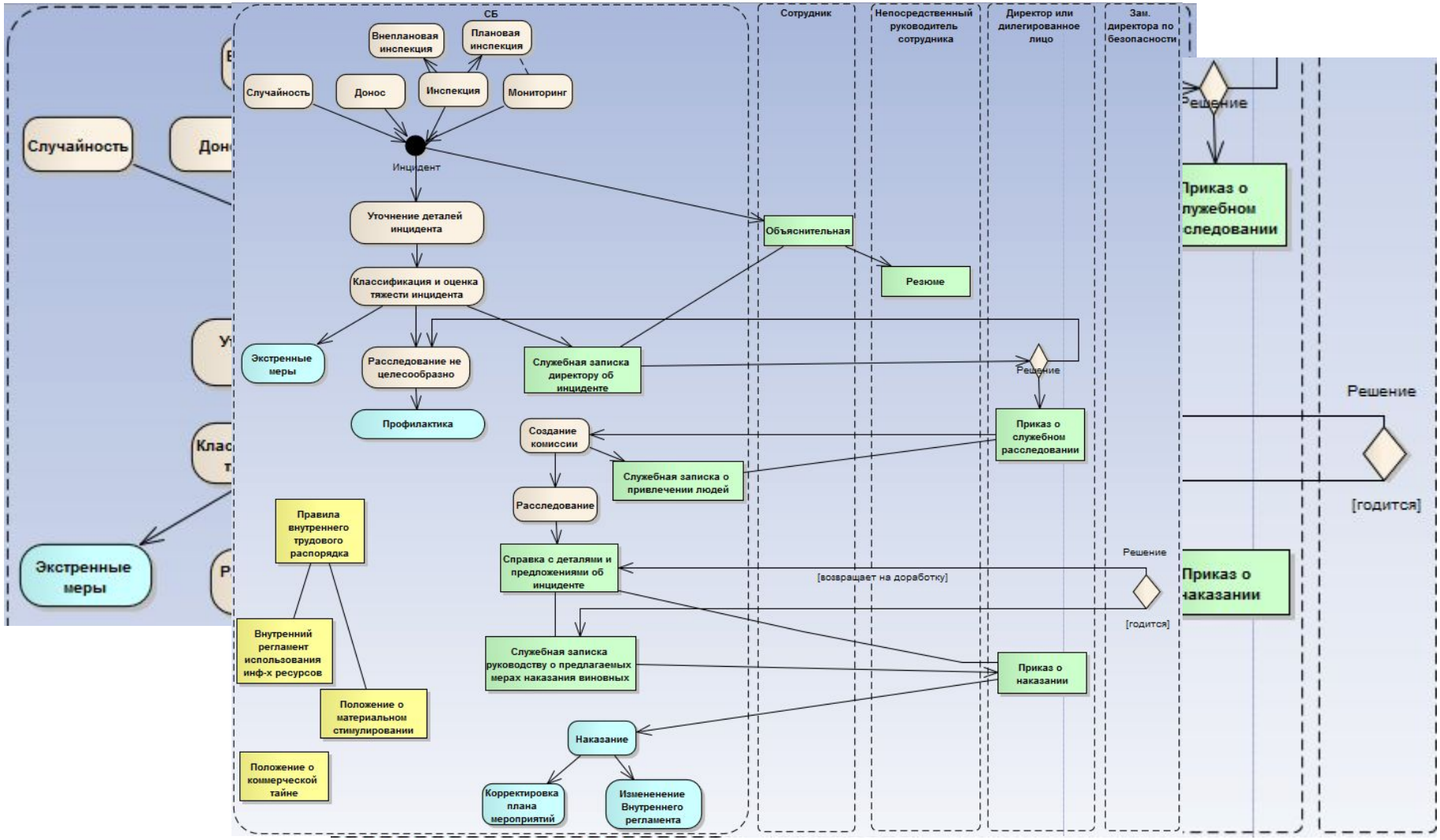


случайные ошибки (InfoWatch)

Инциденты безопасности

3. ВОЗНИК ИНЦИДЕНТ. ЧТО ДЕЛАТЬ?

Процесс управления инцидентами (Incident Management Workflow)



3. РЕГЛАМЕНТЫ отсутствуют или не слишком работают

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ И РАССЛЕДОВАНИЯ

ПОД ПОДПИСЬ:

Сопутствующие работе по инциденту:

- Объяснительная
- Резюме
- Служебная записка об инциденте
- Приказ о расследовании
- Служебная записка о привлечении людей
- Справка с деталями и предложениями об инциденте
- Служебная записка руководству о предлагаемых мерах наказания виновных
- Приказ о наказании
- И другие

3. Инциденту в реальной жизни сопутствует…

… но в DLP системах часто отсутствует

- **ДЕЙСТВИЯ** (включая схемы запросить-разрешить)
  - Уточнить, классифицировать тяжесть, создать комиссию, провести расследование,
  - скорректировать план мероприятий, изменить внутренний регламент..
- **МЕРЫ** (экстренные, профилактика, наказание и т.д.)
- **УДОБСТВО** (действия и решения – реакция «в 1 клик»)
  - задать секретность, связать событие с инцидентом, принять меры и т.п.
- **ИНСТРУКЦИИ и ПОДСКАЗКИ** (что делать, напоминалки)

- **ДЕЛО ПО ИНЦИДЕНТУ** (что произошло и почему)
  - кто, когда, что и как нарушил, какой статус, какие меры приняты, кто был в комиссии, какие были документы, как вел себя сотрудник (признал вину полностью, частично, опроверг, был агрессивен), какое последовало наказание и т.п..
- **ПРОФИЛИ** (пользователя, устройства, конечного узла)
- **МЕТРИКИ ЭФФЕКТИВНОСТИ** (принятых мер, DLP в целом)

4. Учесть человека, регламенты. Увязать с технологиями

АВТОМАТИЗАЦИЯ и УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- **Роли** (не только в UI) и **Иерархии**
- **Политики** (Копи-паст, ссылки и т.п.)
- **События** (расширение, накопление, переоценка по триггеру)
- **Инциденты** (прицеп документов, комментариев, истории действий, Дело)
- **Процессы (Workflow) и Триггеры**
- **Метрики эффективности (KPI)**
- **ТРИАДА:**

1. **Отчеты**
2. **Построитель Запросов (Query Builder)**
3. **Контрольная Панель (Dashboard)**

- **Архивы и доказательная база**
- **Поиск и анализ**

Все **настраиваемое**
Все на **шаблонах**
Все с **предустановками**
Все на **открытых** стандартах
НИЧЕГО ЖЕСТКО ВШИТОГО!

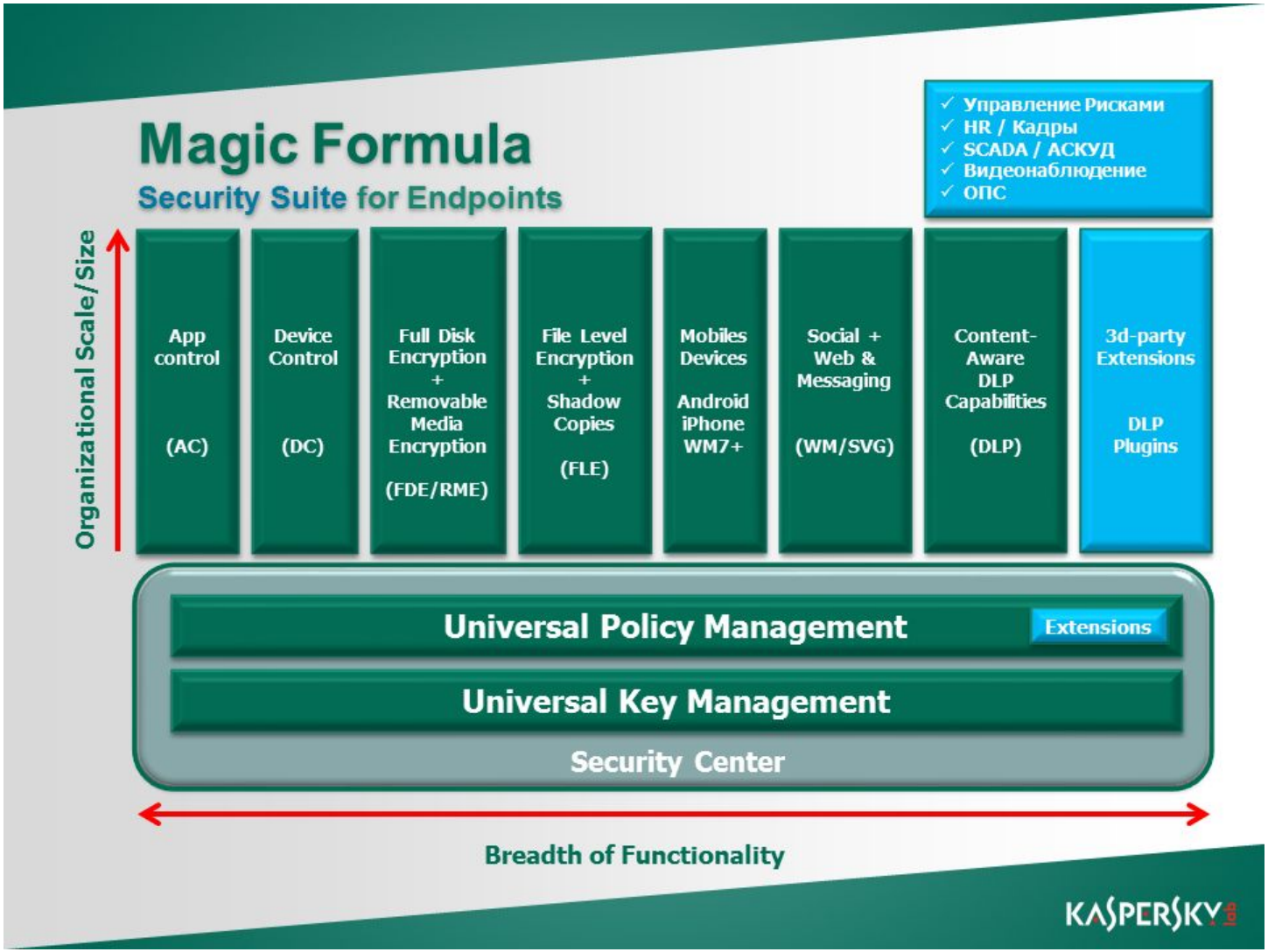
Направление (внос-вынос)
Полномочия (только на чтение)
Ограничения (Limits)

Сигналы тревоги (Alerts)
Уведомления (Notifications)

Обоснования (Justification)
Осведомленность (Awareness)
Прозрачно ли для пользователя

5. ОБЪЕДИНЯЮЩИЙ ИНСТРУМЕНТАРИЙ

ИНТЕГРАЦИЯ, ПОСТОЯННОЕ СОВЕРШЕНСТОВАНИЕ, СИНЕРГИЯ



КАКОЙ МЫ ХОТИМ ВИДЕТЬ ЗАЩИТУ ДАННЫХ

DLP ДОЛЖНА БЫТЬ:

ПРОЩЕ и **ЛЕГЧЕ**

НАДЕЖНЕЕ
и **БЕЗОПАСНЕЕ**

УДОБНЕЕ

ПОНЯТНЕЕ и
ПРЕДСКАЗУЕМЕЕ

ПОЛЕЗНЕЕ
ЭФФЕКТИВНЕЕ

ШИРЕ ДЕШЕВЛЕ

DLP ДОЛЖНА НАМ ДАТЬ:

ПРОСТОТА.

СПОКОЙСТВИЕ.

БЕЗОПАСНОСТЬ. НАДЁЖНОСТЬ.

УВЕРЕННОСТЬ.

ДОВЕРИЕ.

ГАРМОНИЯ И КРАСОТА.

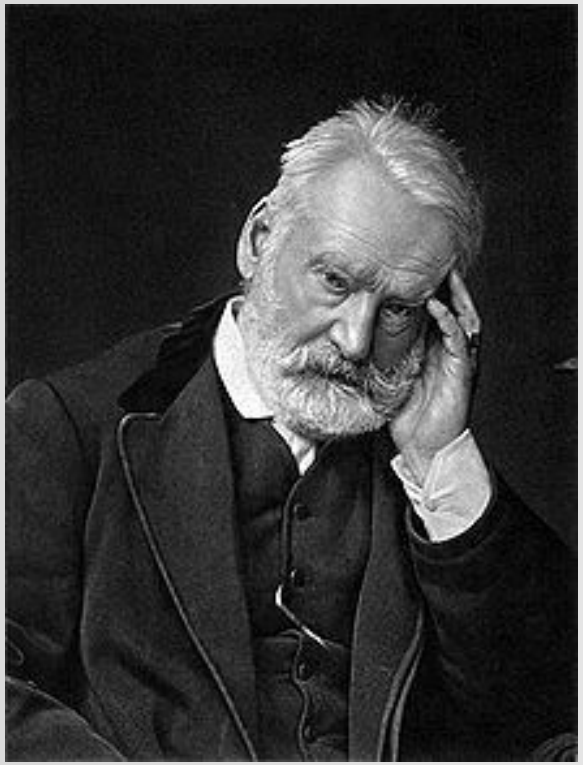
КОМФОРТ.

ПОЛЬЗА.

УДОВОЛЬСТВИЕ!

Data *Luxury* Protection (DLP) – защита данных
с удовольствием!

Data *Luxury* Protection (DLP) – защита данных *с удовольствием!*



Ничто не поражает с такой силой как роскошь, когда её видишь первый раз

Виктор Гюго. Человек, который смеётся.

Luxury ['lʌgʒ(ə)rɪ], ['lʌkʃ(ə)rɪ] **(англ.)**

1. Роскошь, богатство
2. **Наслаждение, большое удовольствие**

Gabrielle Bonheur "Coco" Chanel о роскоши

Обещанный ответ

РОСКОШЬ — ЭТО КОГДА ИЗНАНКА ТАК ЖЕ КРАСИВА, КАК И ЛИЦО.

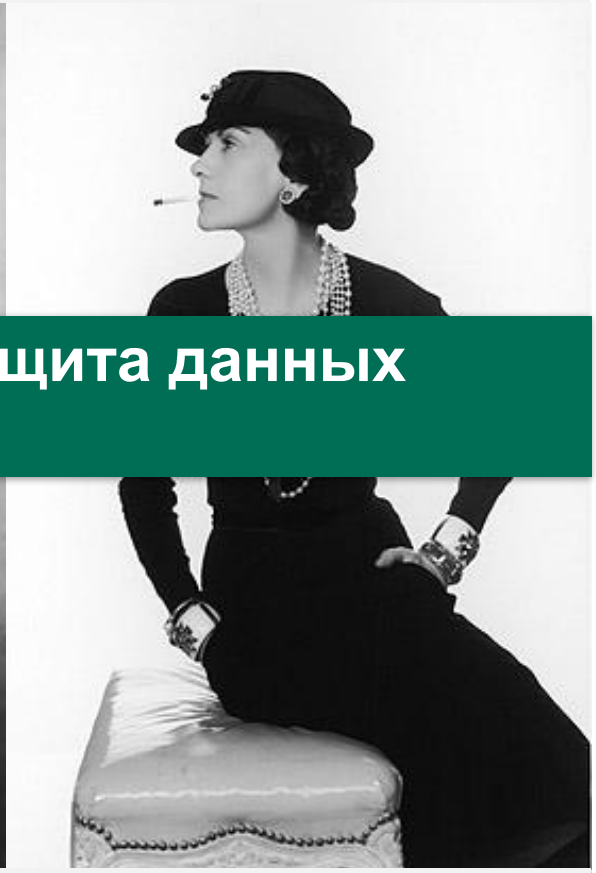
Коко Шанель

РОСКОШЬ ДОЛЖНА БЫТЬ УДОБНОЙ, ИНАЧЕ ЭТО НЕ РОСКОШЬ.

Коко Шанель

Gabrielle Bonheur "Coco" Chanel о DLP

DLP — ЭТО КОГДА ИЗНАНКА ТАК ЖЕ КРАСИВА, КАК И ЛИЦО.
Коко Шанель, из неопубликованного



Data *Luxury* Protection (DLP) – защита данных
с удовольствием!

DLP ДОЛЖНА БЫТЬ УДОБНОЙ, ИНАЧЕ ЭТО НЕ DLP.
Коко Шанель, из неопубликованного

Data *Luxury* Protection (DLP) – защита данных *с удовольствием!*

Спасибо за внимание!

Есть вопрос?
Контакт для связи:

DLP Research, R&D, Kaspersky Lab

28 октября 2011

InfoProstranstvo, Moscow

IV международная конференция

DLP-Russia

Protect your inner space

KASPERSKY lab

Luxury (англ.) - Роскошь

БОНУС. Цитаты Коко Шанель о роскоши

- Роскошь должна быть удобной, иначе это не роскошь.
- Роскошь - это когда изнанка так же красива, как и лицо.
- Роскошь и скромность — две сестры.
- Роскошь — это необходимость, которая начинается там, где заканчивается необходимость.
- Роскошь - это не вызов бедности, это вызов вульгарности.
- Принято считать, что роскошь — противоположность нищеты. Нет, роскошь — противоположность вульгарности.