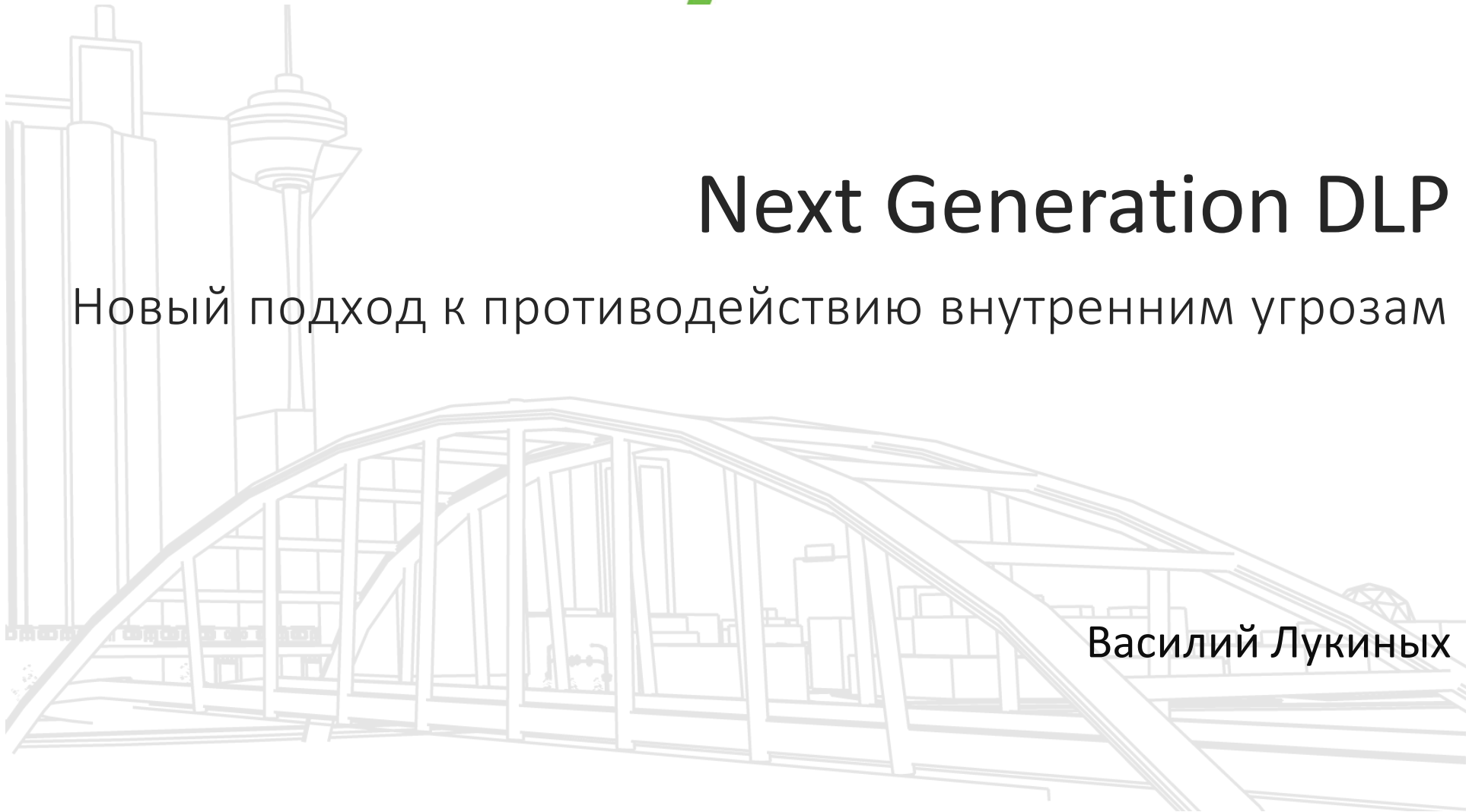
ДиалогНаука

SOLAR SECURITY
software&services



Next Generation DLP

Новый подход к противодействию внутренним угрозам

Василий Лукиных

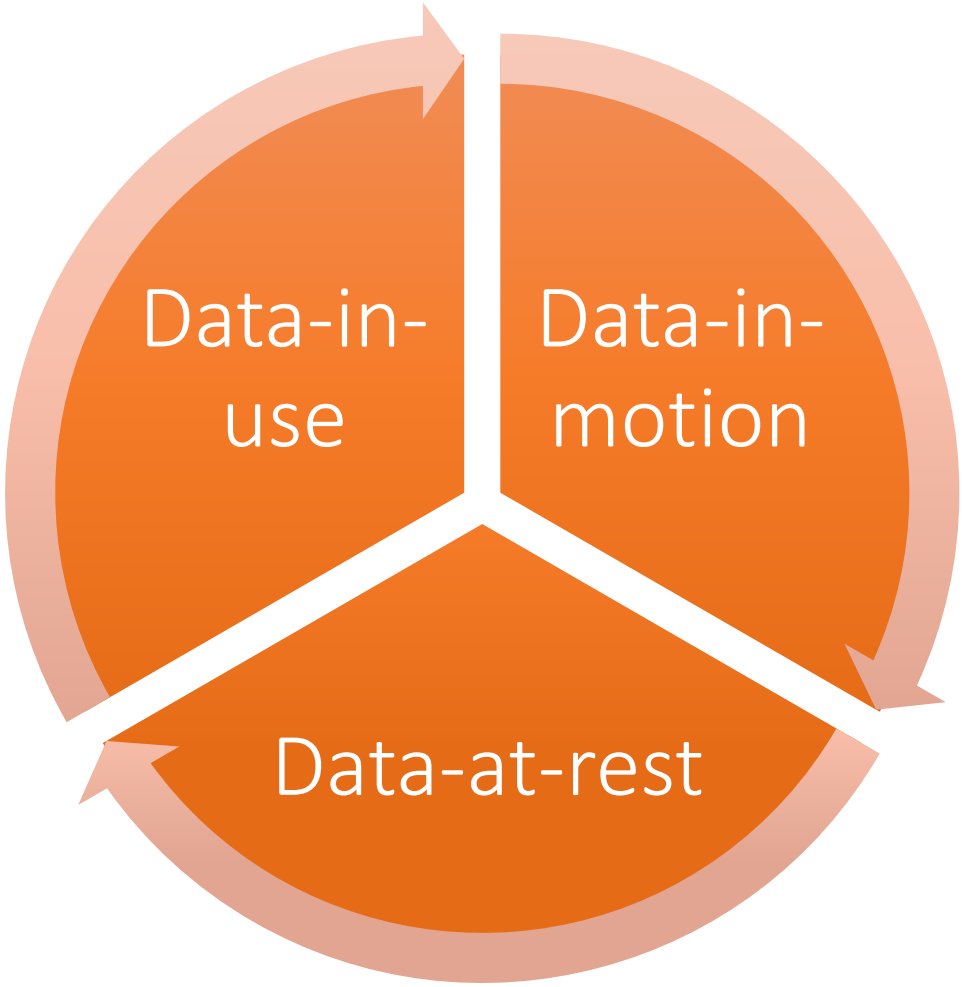
25 апреля 2017 г.

Agenda

1. Классический подход к DLP: data-centric
2. Тренды DLP: рынок и отрасль
3. Next Generation DLP: data-driven & people-centric
4. Это работает

1. Немного истории

1.1 Классический подход к DLP



1.2 Контроль коммуникаций

Dozor Mail Connector

Почтовый трафик

Web Proxy

Доступ пользователей

Dozor Traffic Agent

Сетевой трафик

Dozor Endpoint Agent

Действия пользователей

Dozor File Crawler

Файлы в сети

Dozor Core

Фильтрация
Хранение
События и инциденты
Информационные объекты
Единое управление

Profile & Anomaly

Досье
Аналитические инструменты

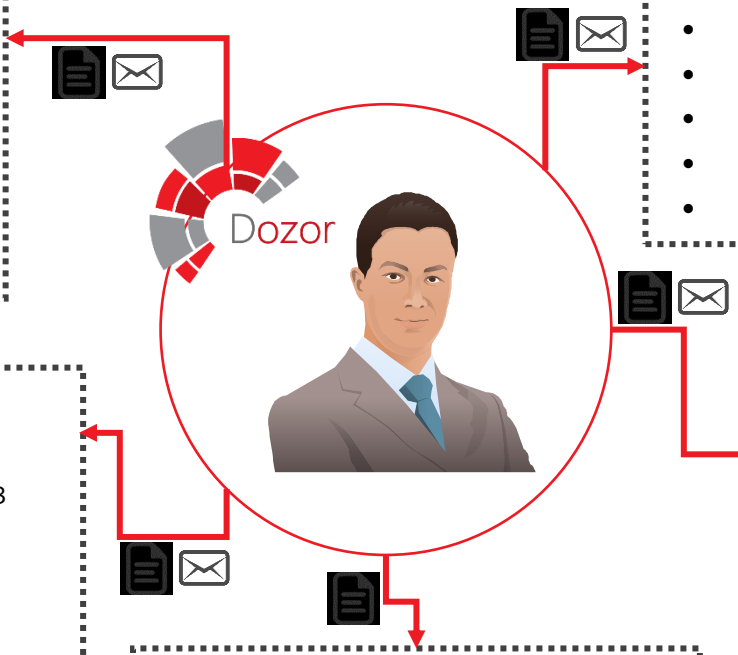
Long-Term Archive

Долгосрочное хранение

Информационная и экономическая безопасность

1.3 Каналы коммуникаций

МОНИТОРИНГ + БЛОКИРОВКА



Корпоративная почта

- Microsoft Exchange
- IBM Lotus Notes
- CommuniGate

Веб-почта

- Mail.ru, Gmail, Yandex, 40+ доменов

Мессенджеры

- OSCAR - ICQ, QIP
- MMP - Mail.Ru Агент
- MSN - Windows Live Messenger
- XMPP - Google Talk, Jabber
- IRC, Yahoo messenger
- Skype, MS Lync

Интернет-трафик

- Сообщения и файлы через HTTP(S)
- Файлы через FTP, FTP over HTTP, WebDAV

Интернет-сервисы

- Социальные сети
- Форумы, блоги
- Сайты поиска работы
- POST-запросы

Аудит файловых хранилищ

- Рабочие станции
- Сетевые хранилища

Внешние устройства

- Копирование и чтение
- …

Печать

- Локальные и сетевые принтеры

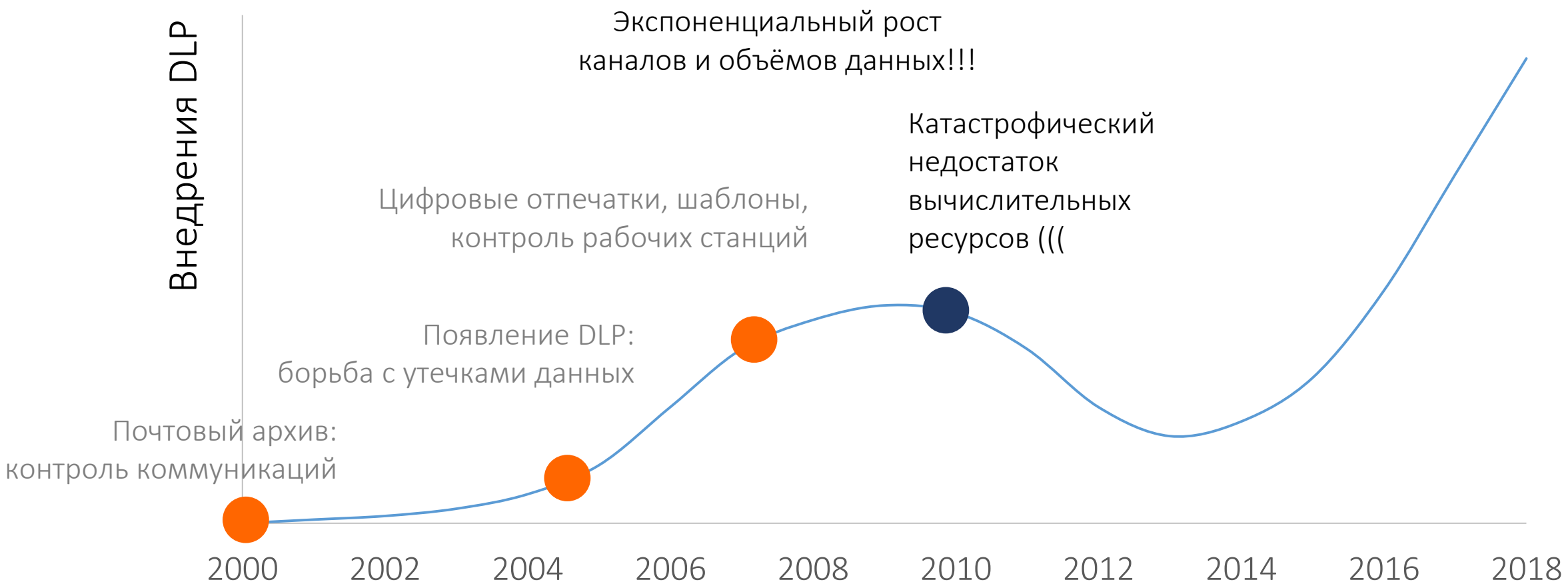
Контроль приложений

- Облака Dropbox, Yandex.Disk и пр
- Любые приложения
- Буфер обмена

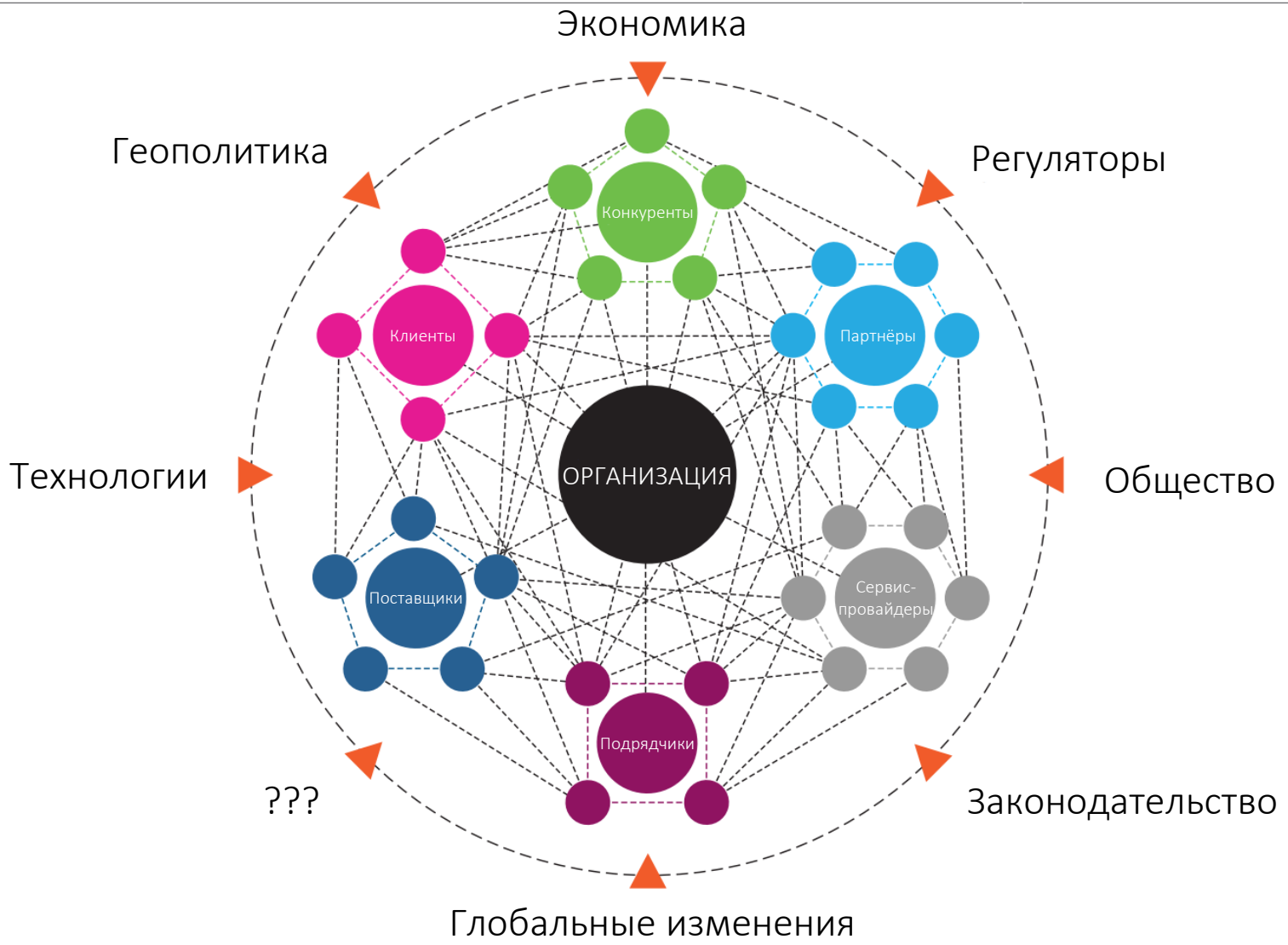
1.4 «Классические» DLP

- Предотвращение утечек информации
- Контроль коммуникаций сотрудников

2. Вернёмся к истории: драйверы



2.1 Мир без периметра!



- Постоянное взаимодействие
- Информационные потоки – кровь бизнеса
- Рост значимости для бизнеса и самих данных, и значимость безопасности данных

2.2 А мы точно защищаем данные?

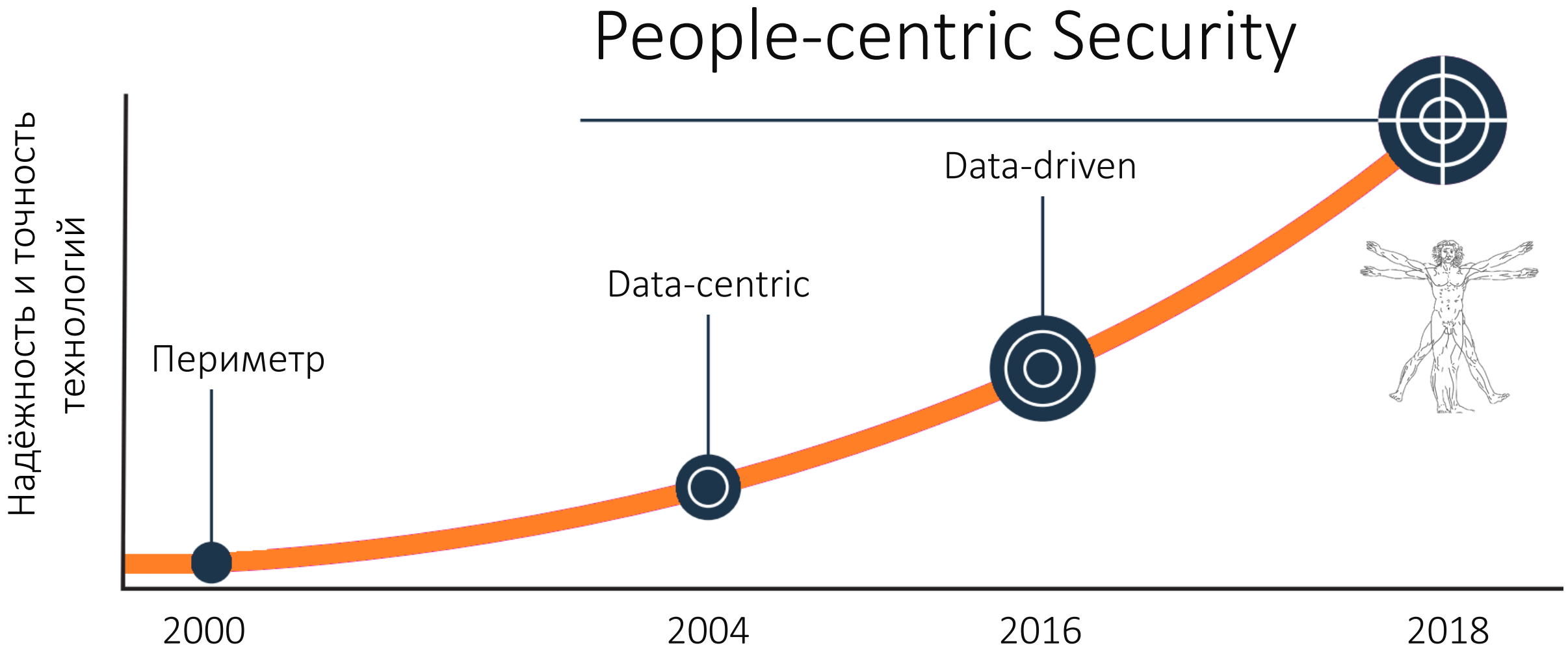
2.3 И за угрозами для бизнеса стоят люди

2.4 Все дороги ведут…

Безопасность через мониторинг

People-centric Security

3. Next Generation DLP



3.1 Новые вызовы и возможности DLP

а) Контроль информационных потоков

- Где реально хранится информация?
- А где и как обрабатывается?
- Кому и что реально передается?

3.1 Новые вызовы и возможности DLP

б) Выявление и мониторинг групп риска

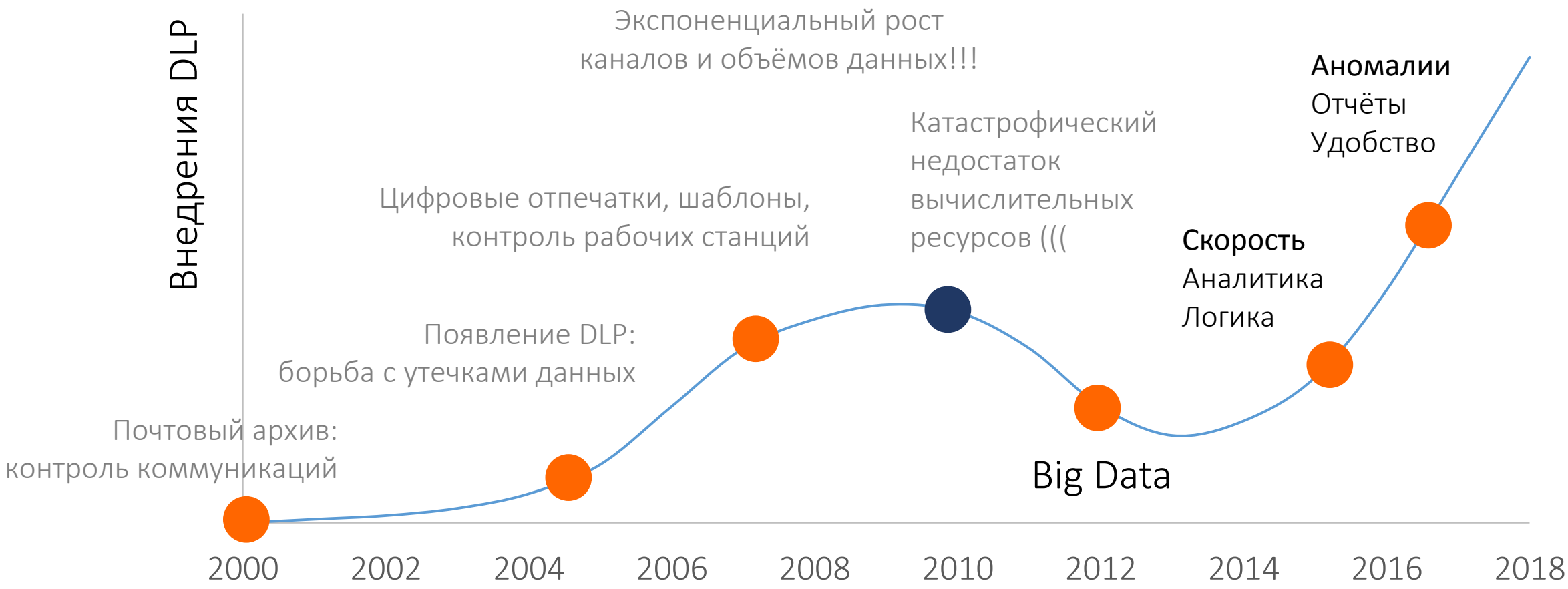
- Группы риска: поиск работы, игроманы, должники, неадекватные траты
- Компрометирующие связи: конкуренты, криминал, аффилированность
- Конфликты: производственные, личные
- Аномалии поведения: связи, каналы коммуникаций, профиль нарушений

3.1 Новые вызовы и возможности DLP

в) Выявление и расследование мошеннических схем

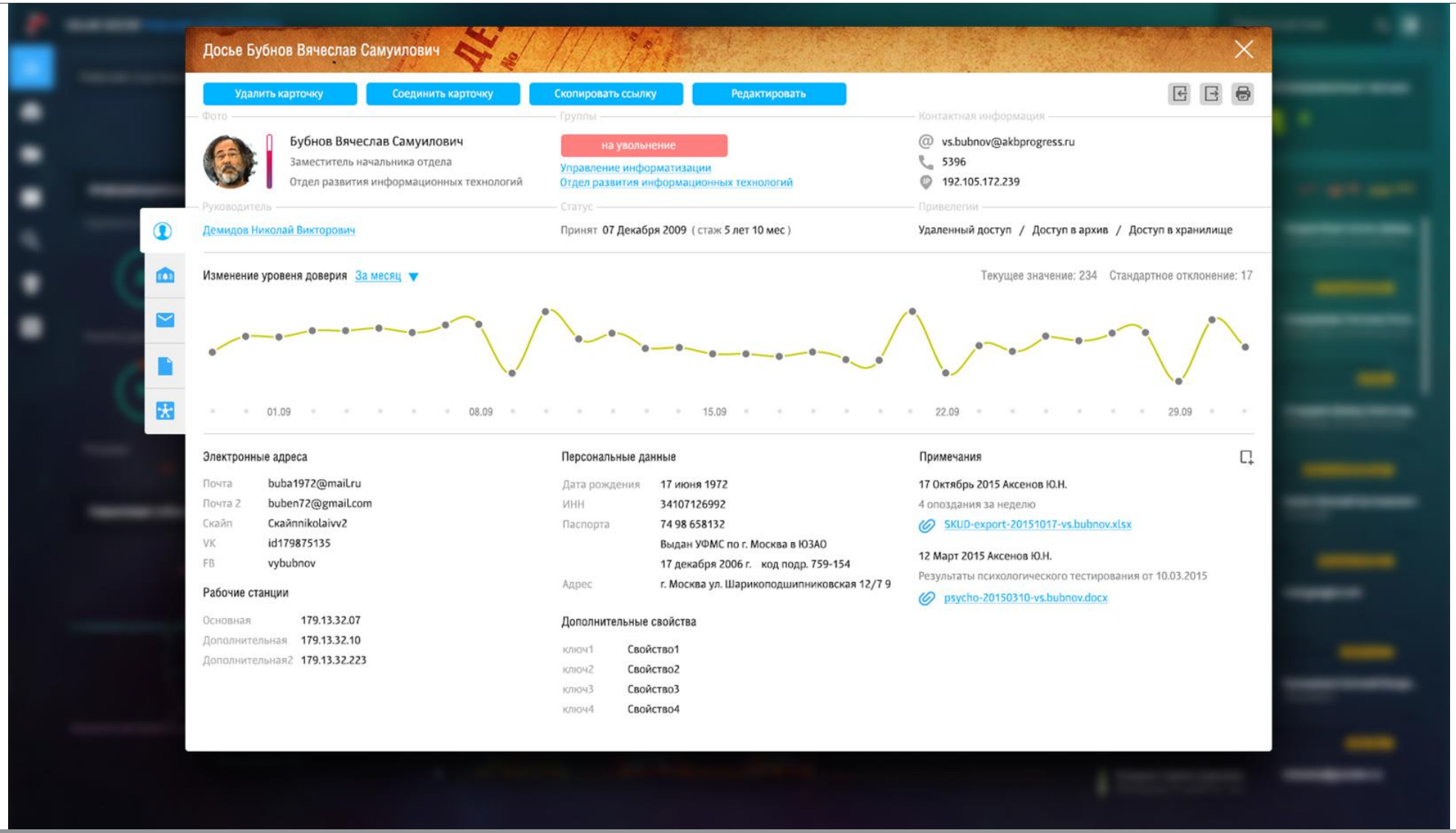
- Выявление косвенных признаков мошеннических схем
- Анализ аномалий коммуникаций
- Расследование, проверка гипотез

3.2 Что в ответ?

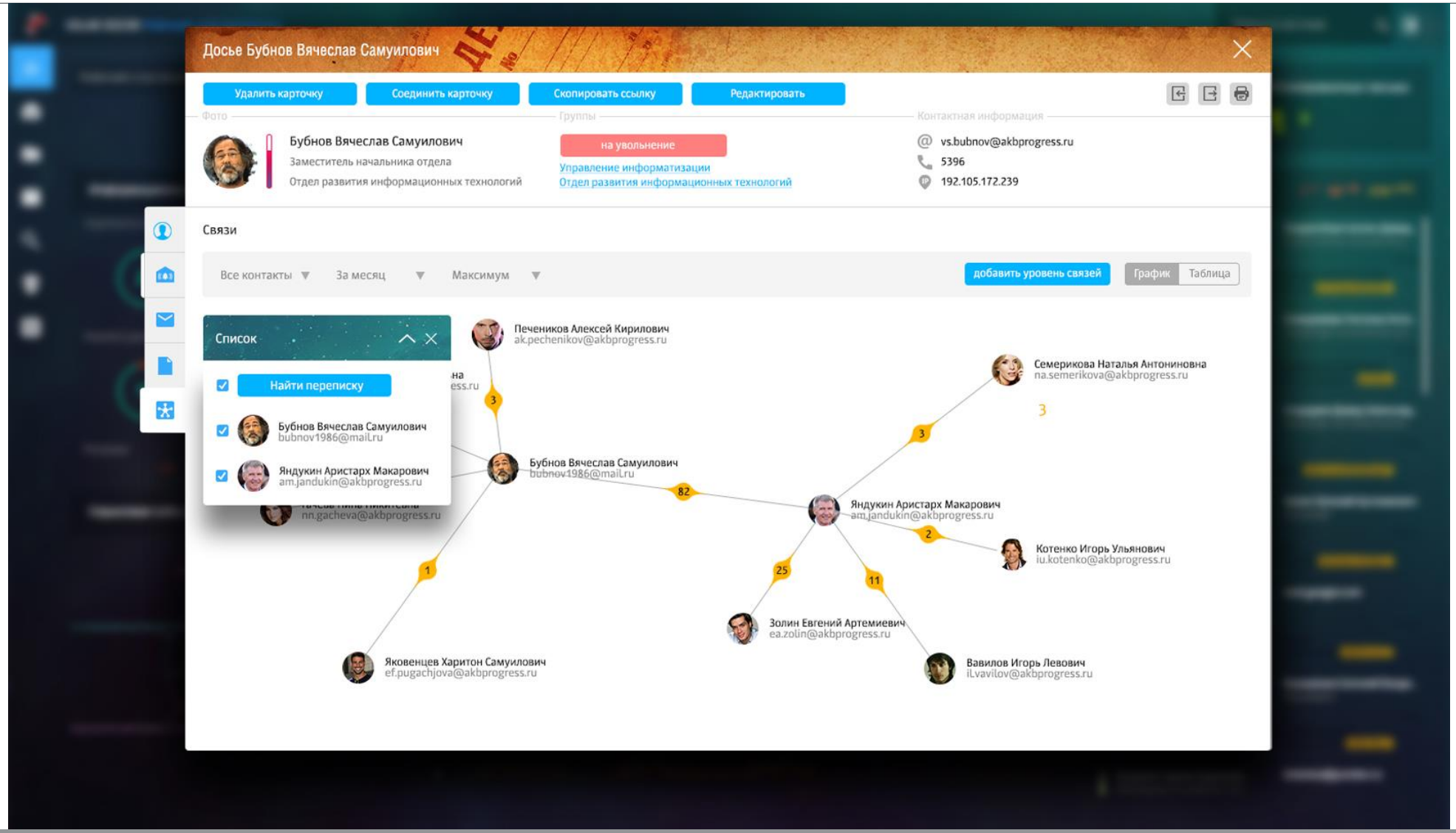


3.3 Три фокуса внимания

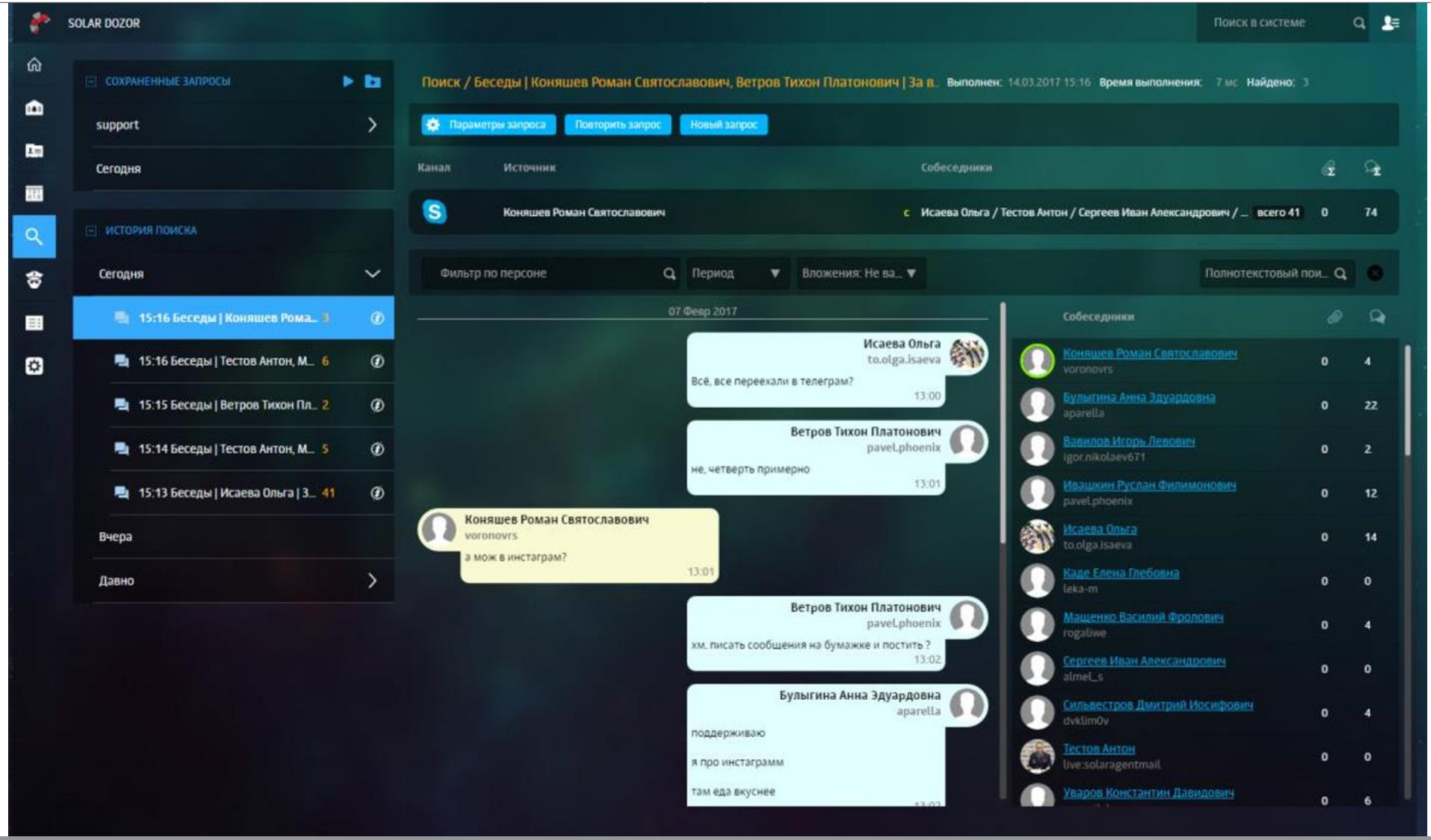
3.4 Досье 360°: аномалии



3.4 Досье 360°: связи и коммуникации



3.4 Досье 360°: мгновенный доступ



3.4 Досье 360°: «Что у нас есть на Васю?»

3.5 Next Generation DLP

- Предотвращение утечек информации
- Контроль коммуникаций сотрудников
- Выявление и мониторинг групп риска
- Выявление признаков мошенничества
- Анализ аномалий коммуникаций
- Досье на персону
- Проведение расследований
- Контроль информационных потоков

Solar Dozor

система контроля коммуникаций сотрудников, выявления признаков корпоративного мошенничества и проведения расследований

4. Что дальше?..


MSSP
UEBA
Cloud
Внедрения DLP
Экспоненциальный рост
каналов и объёмов данных!!!
Аномалии
Отчёты
Удобство
Катастрофический
недостаток
вычислительных
ресурсов (((
Цифровые отпечатки, шаблоны,
контроль рабочих станций
Скорость
Аналитика
Логика
Появление DLP:
борьба с утечками данных
Почтовый архив:
контроль коммуникаций
Big Data
2000
2002
2004
2006
2008
2010
2012
2014
2016
2018

Узнайте больше про Solar Dozor!

Контакты ДиалогНаука:
marketing@DialogNauka.ru
8 (495) 980-67-76

Василий Лукиных
Менеджер по развитию бизнеса
Solar Security
V.Lukinykh@solarsecurity.ru
+7 915 303 00 08