

# ДиалогНаука



## Next Generation DLP

Новый подход к противодействию внутренним угрозам

Василий Лукиных



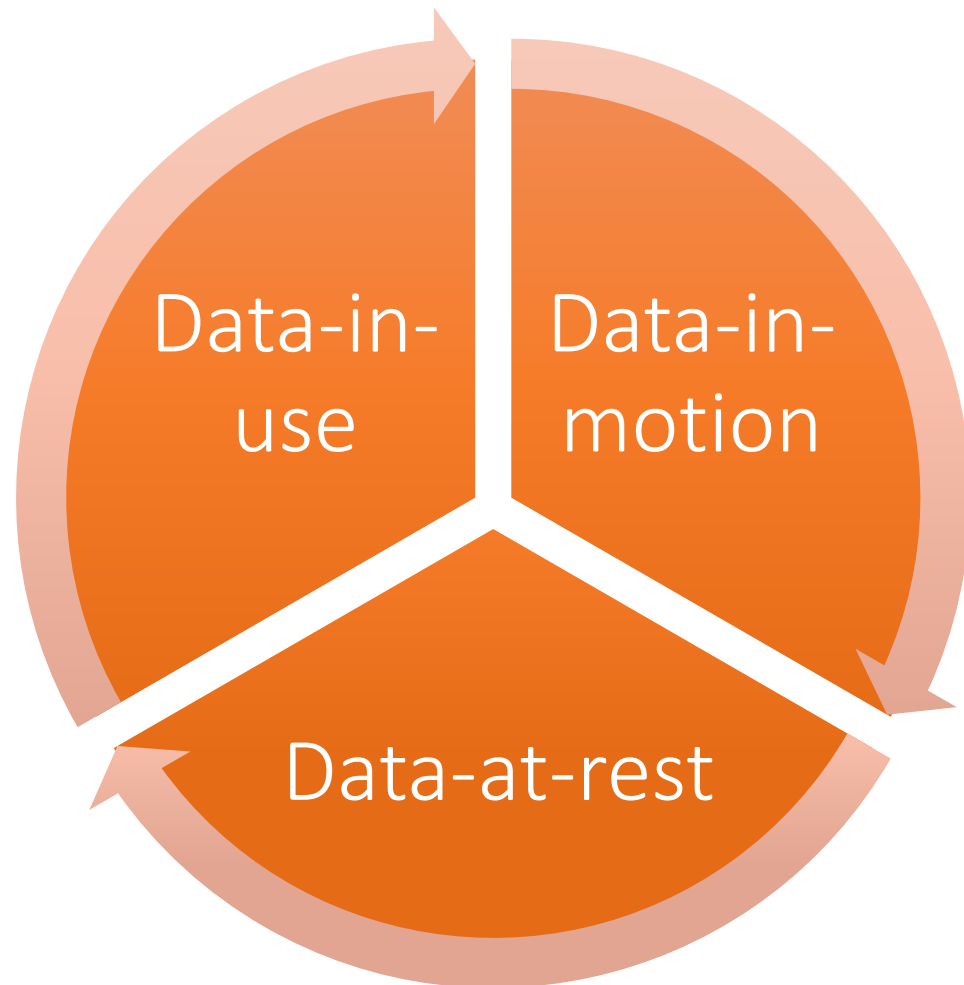
# Agenda

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

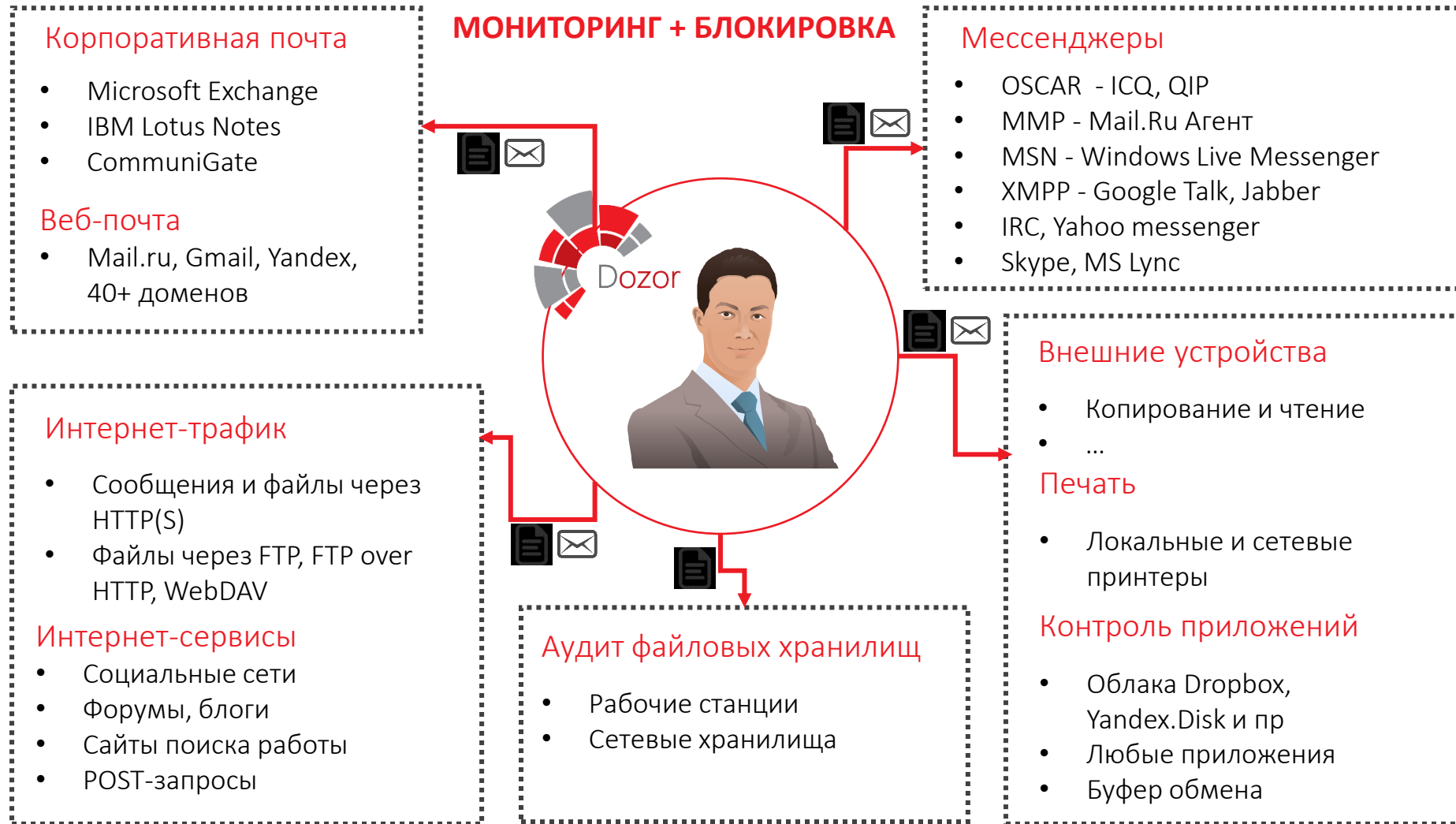
Long-Term  
Archive

Долгосрочное хранение



Информационная  
и экономическая  
безопасность

# 1.3 Каналы коммуникаций

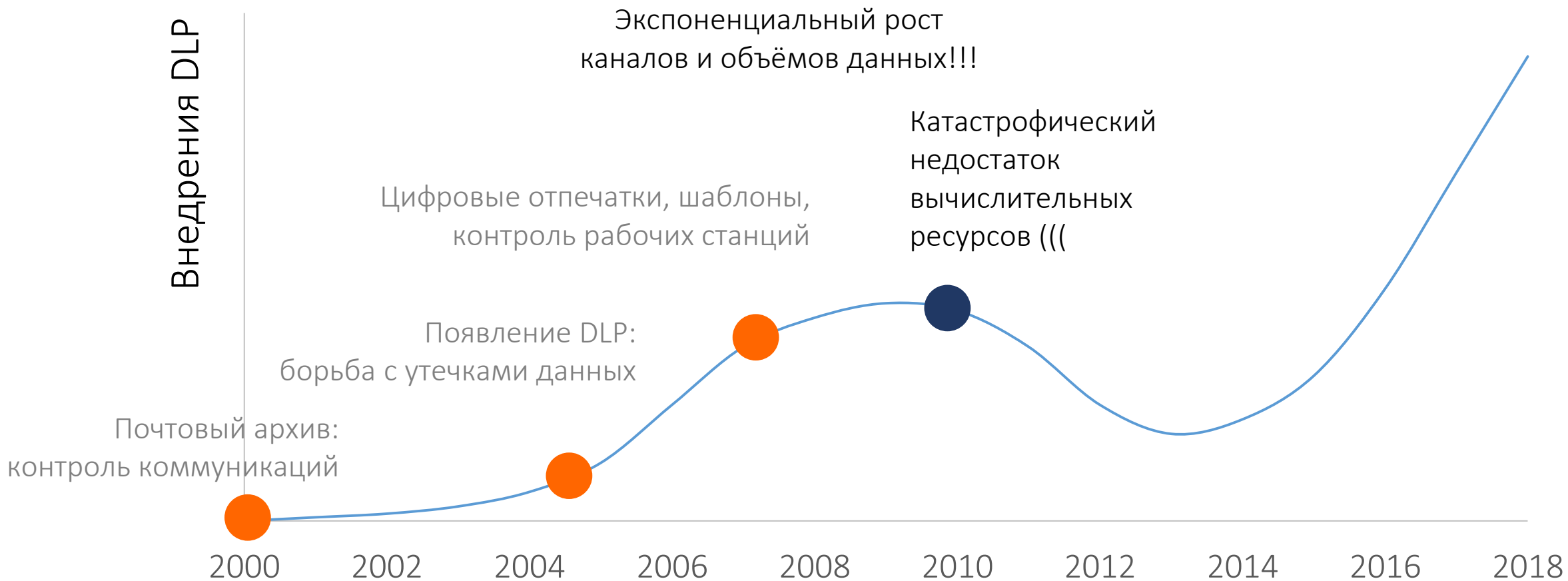




## 1.4 «Классические» DLP

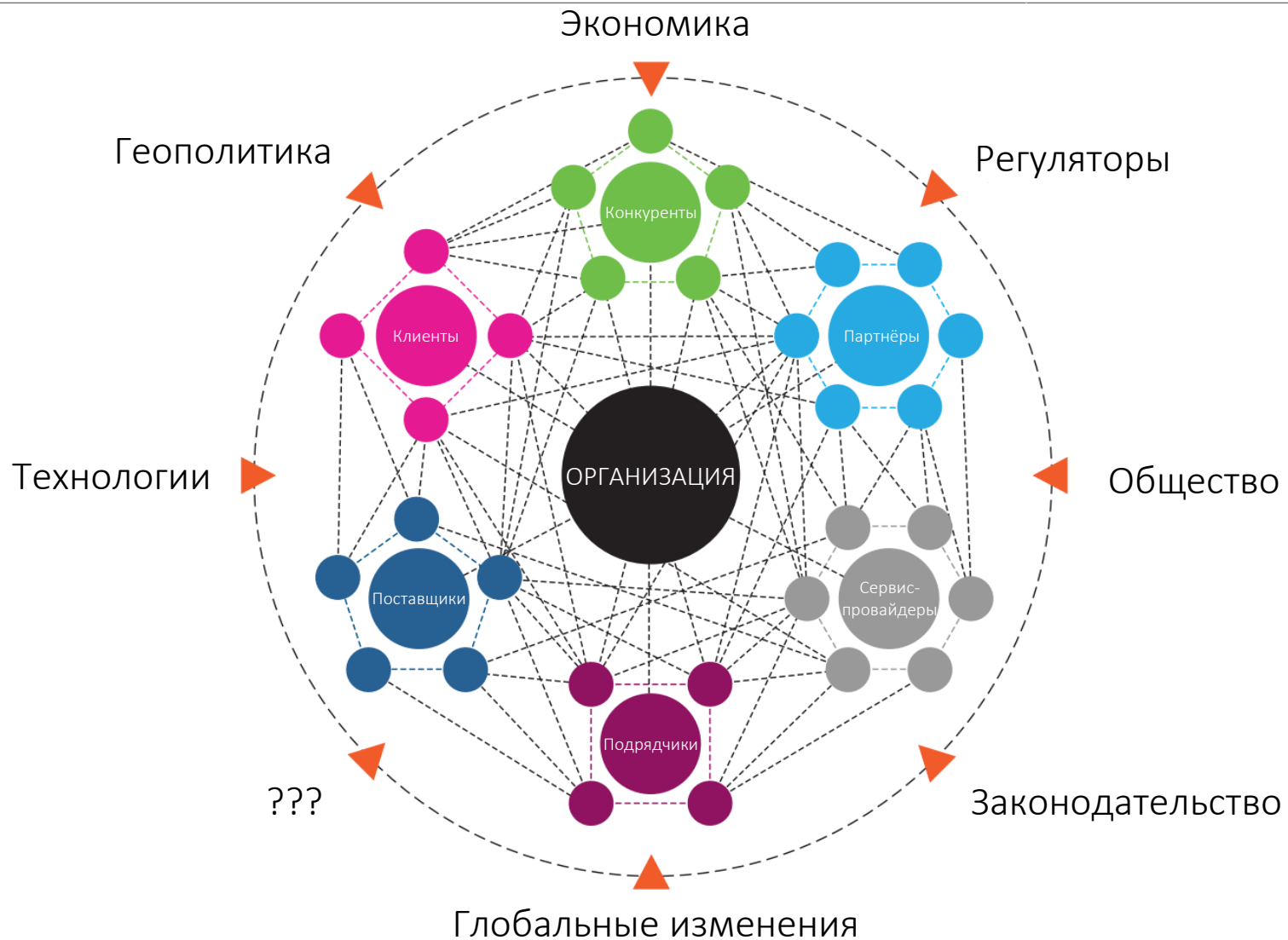
- Предотвращение утечек информации
- Контроль коммуникаций сотрудников

## 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...

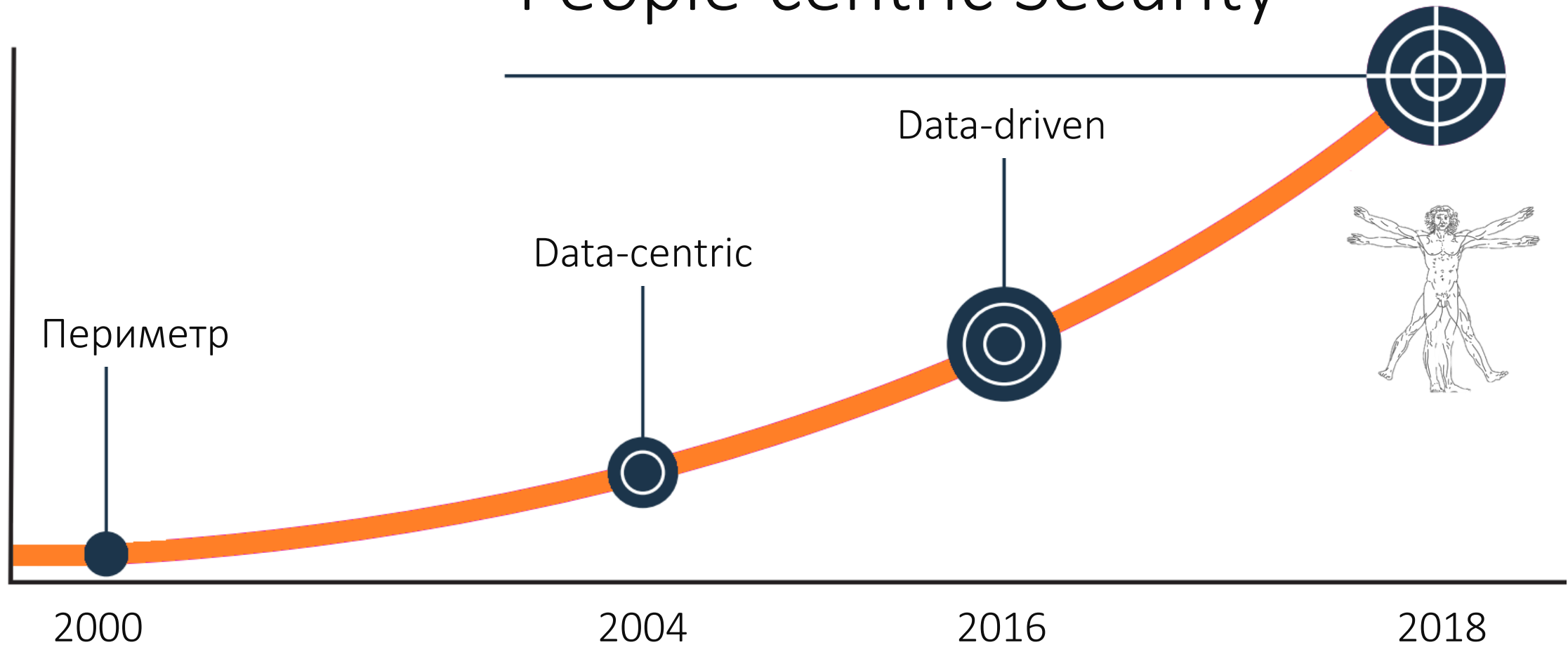
Безопасность через **мониторинг**

**People-centric** Security

# 3. Next Generation DLP

## People-centric Security

Надёжность и точность  
ТЕХНОЛОГИЙ





# 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

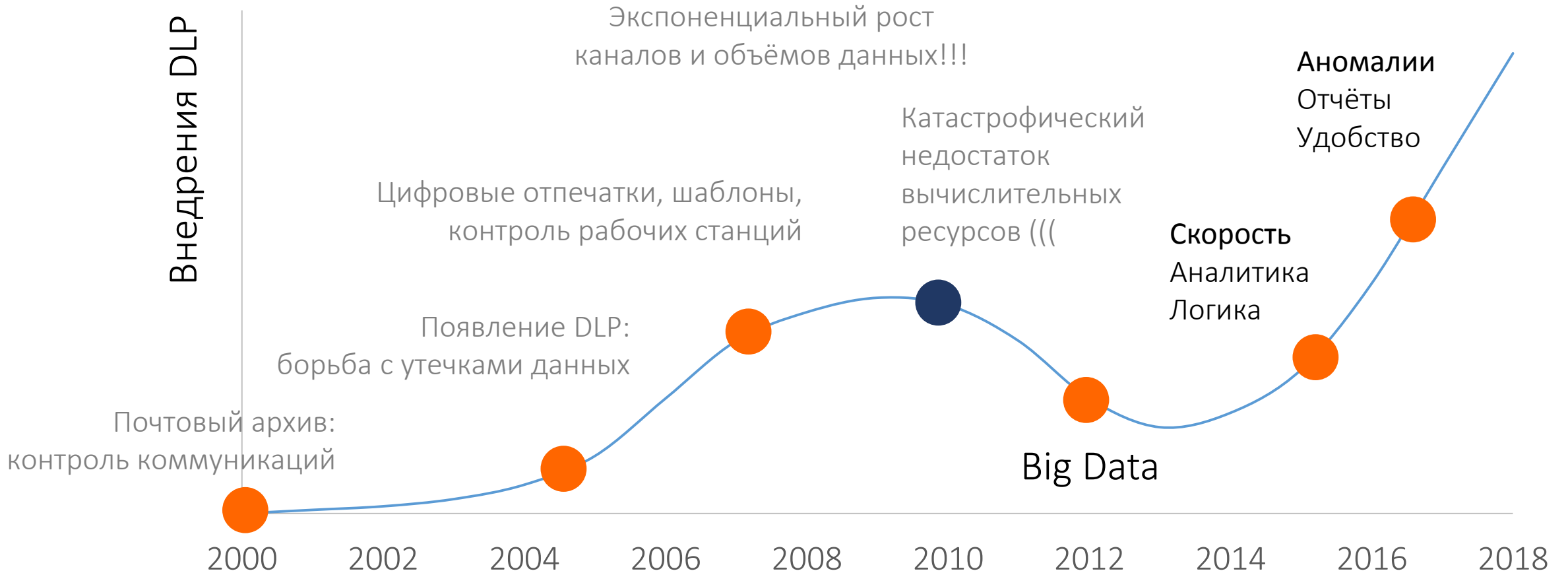
## в) Выявление и расследование мошеннических схем

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

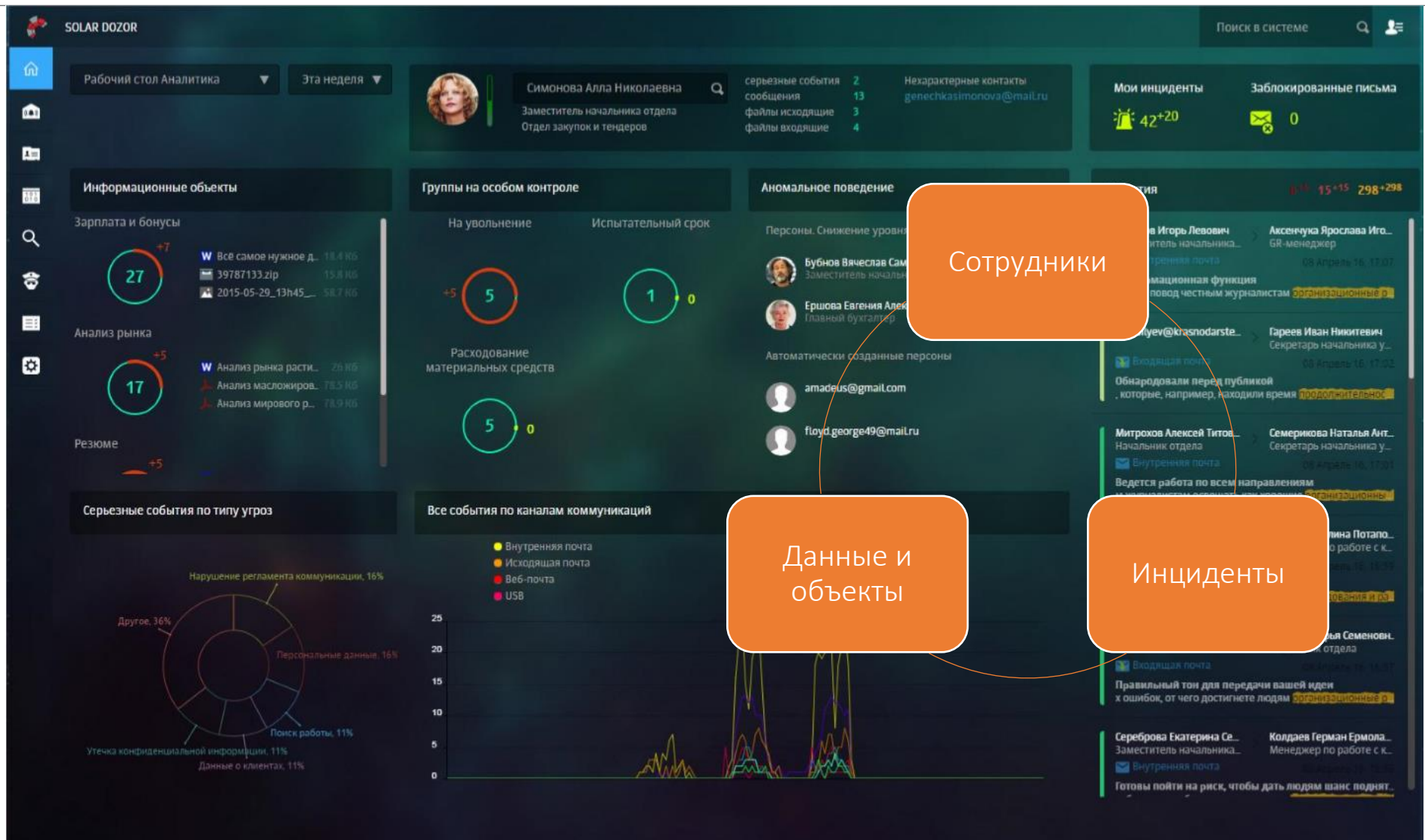




## 3.2 Что в ответ?



# 3.3 Три фокуса внимания



The screenshot shows the SOLAR DOZOR dashboard interface. Three orange callout boxes are overlaid on the dashboard, each connected to a specific area of the interface by a thin line:

- Сотрудники (Employees):** This box points to the 'Персоналии' (Personnel) section, which lists employees like 'Бубнов Вячеслав Сам...' and 'Ершова Евгения Алекс...'. It also points to the 'Аномальное поведение' (Anomalous behavior) section.
- Данные и объекты (Data and Objects):** This box points to the 'Информационные объекты' (Informational objects) section, which includes charts for 'Зарплата и бонусы' (Salary and bonuses) and 'Анализ рынка' (Market analysis).
- Инциденты (Incidents):** This box points to the 'Мои инциденты' (My incidents) and 'Заблокированные письма' (Blocked emails) sections on the right side of the dashboard.


# 3.4 Досье 360°: аномалии

**Досье Бубнов Вячеслав Самуилович**

Удалить карточку | Соединить карточку | Скопировать ссылку | Редактировать

---

**Фото**



**Бубнов Вячеслав Самуилович**  
Заместитель начальника отдела  
Отдел развития информационных технологий

**Группы**

на увольнение

Управление информатизации  
Отдел развития информационных технологий

**Контактная информация**

vs.bubnov@akbprogress.ru  
5396  
192.105.172.239

---

**Руководитель**

Демидов Николай Викторович

**Статус**


Принят 07 Декабря 2009 ( стаж 5 лет 10 мес )

**Привилегии**

Удаленный доступ / Доступ в архив / Доступ в хранилище

---

**Изменение уровня доверия** За месяц ▼ Текущее значение: 234 Стандартное отклонение: 17




---

**Электронные адреса**

Почта buba1972@mail.ru  
Почта 2 buben72@gmail.com  
Скайп Скайпnikolaivv2  
VK id179875135  
FB vyubnov

**Рабочие станции**

Основная 179.13.32.07  
Дополнительная 179.13.32.10  
Дополнительная2 179.13.32.223

**Персональные данные**

Дата рождения 17 июня 1972  
ИНН 34107126992  
Паспорта 74 98 658132  
Выдан УФМС по г. Москва в Ю3АО  
17 декабря 2006 г. код подр. 759-154  
Адрес г. Москва ул. Шарикоподшипниковская 12/7 9

**Дополнительные свойства**

ключ1 Свойство1  
ключ2 Свойство2  
ключ3 Свойство3  
ключ4 Свойство4

**Примечания**

17 Октябрь 2015 Аксенов Ю.Н.  
4 опоздания за неделю  
[SKUD-export-20151017-vs.bubnov.xlsx](#)  
12 Март 2015 Аксенов Ю.Н.  
Результаты психологического тестирования от 10.03.2015  
[psycho-20150310-vs.bubnov.docx](#)

solaresecurity.ru

+7 (499) 755-07-70

19

# 3.4 Досье 360°: связи и коммуникации

Досье Бубнов Вячеслав Самуилович

Удалить карточку | Соединить карточку | Скопировать ссылку | Редактировать

Фото: Бубнов Вячеслав Самуилович  
Заместитель начальника отдела  
Отдел развития информационных технологий

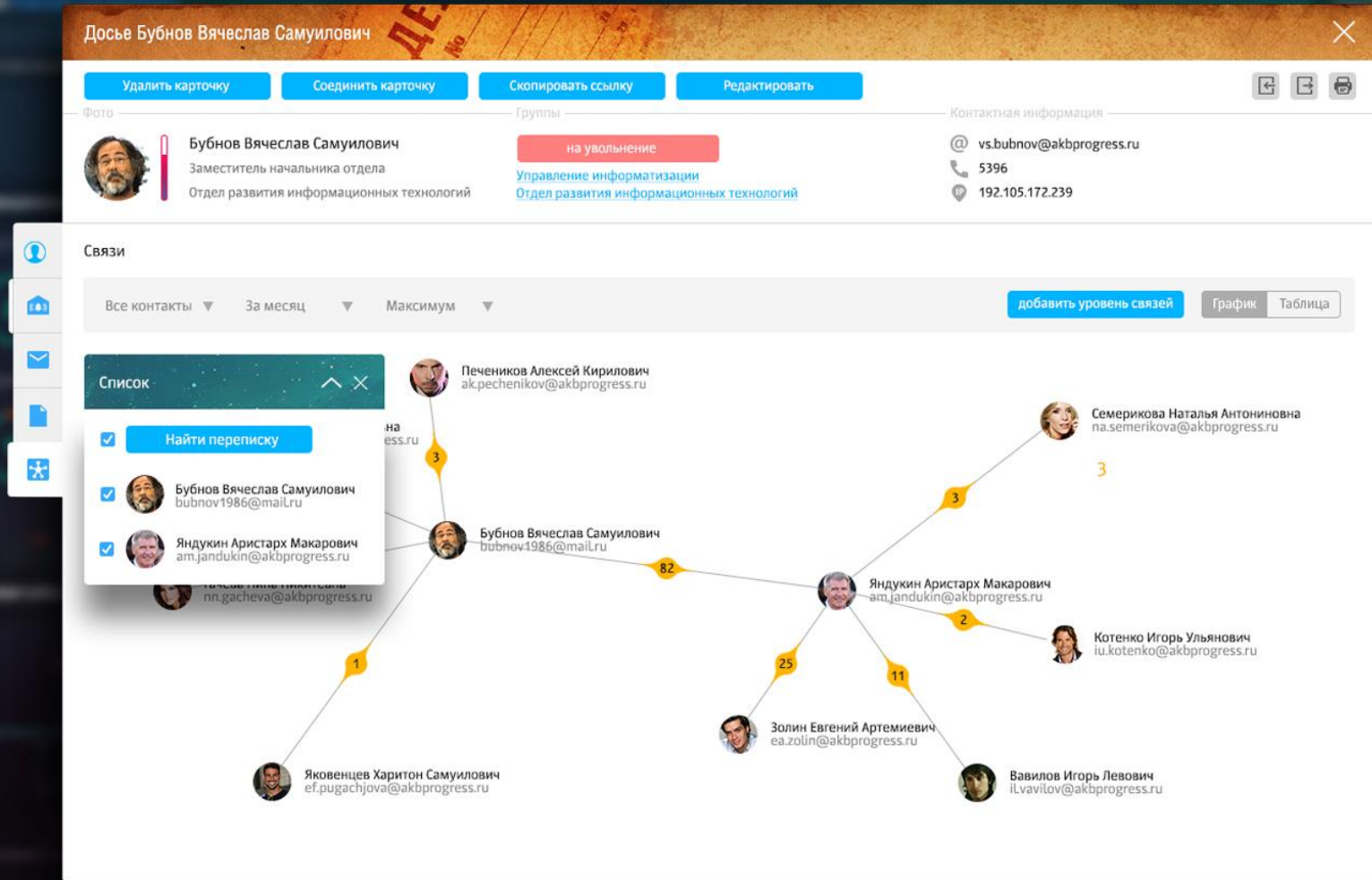
Группы: на увольнение  
Управление информатизации  
Отдел развития информационных технологий

Контактная информация: @ vs.bubnov@akbprogress.ru, 5396, 192.105.172.239

Связи: Все контакты | За месяц | Максимум | добавить уровень связей | График | Таблица

Список: Найти переписку

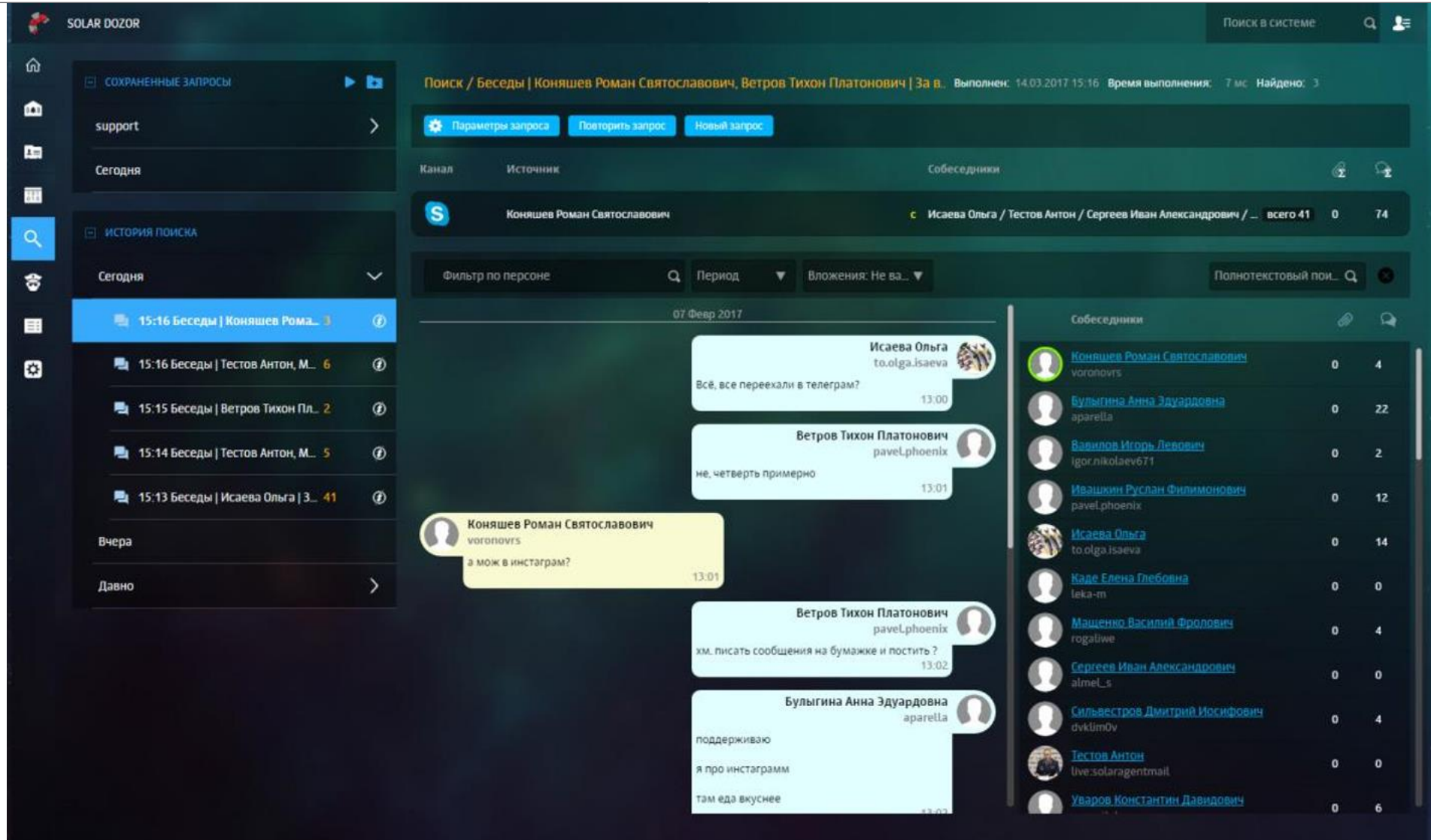
- Бубнов Вячеслав Самуилович (bubnov1986@mail.ru)
- Яндукин Аристарх Макарович (am.jandukin@akbprogress.ru)



```
graph LR; A[Яндукин Аристарх Макарович] ---|82| B[Бубнов Вячеслав Самуилович]; A ---|3| C[Семерикова Наталья Антоиновна]; A ---|2| D[Котенко Игорь Ульянович]; A ---|25| E[Золин Евгений Артемиевич]; A ---|11| F[Вавилов Игорь Левович]; B ---|1| G[Яковенцев Харитон Самуилович]; C ---|3| H[Печеников Алексей Кирилович]; G ---|1| I[Яковенцев Харитон Самуилович];
```



# 3.4 Досье 360°: мгновенный доступ



The screenshot displays the SOLAR DOZOR interface. On the left, there is a sidebar with navigation options: СОХРАНЕННЫЕ ЗАПРОСЫ (Saved Requests) and ИСТОРИЯ ПОИСКА (Search History). The main area shows search results for a specific channel: 'Коняшев Роман Святославович'. The search results include a list of conversations with their respective counts and timestamps. The selected conversation is expanded, showing a chat history with messages from participants like Исаева Ольга, Ветров Тихон Платонович, and Булыгина Анна Эдуардовна. The interface also includes a search bar at the top right and a list of participants on the right side.

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

Поиск в системе

**Сводный отчет по персоне** За период: 22.10.2016 - 21.11.2016 Выполнен: 21.11.2016 13:11

**Машенко Василий Фролович**

Имя - должность - отдел

Секретарь начальника управления

Учетно-операционное управление

руководитель

**Седов Варфоломей Иосифович**

Испытательный срок

Президент банка - Пре...

Вице-президент - Руководитель фронт-офиса

Учетно-операционное упра...

контактная информация

vf.mashenko@akb... 192.168.10.27

+7 499 789 63 21 +7 916 247 88 96

7422

привилегии

smb:\\1c-8.2\otchet\IT\ - чтение и запись

**События и инциденты**



2016 Авг 29 Сент 12 Сент 26 Окт 10 Окт 24 2016 Новб 07

инциденты события

**Связи** Кол-во сообщ. Персон из ОШС

Внешняя корпоративная почта		
g.dobrodeev@wecompany.com	100	3
p.salnikov@wecompany.com	90	17
Веб-почта		
garik987@email.com	72	3
freeew@mymail.com	19	5
Мессенджеры		
nakazator333	16	9
darklord23	27	3

**Коммуникации**

Информационный объект	22	11	4	6	43
Информационный объект 2	17	10	7	5	42
Информационный объект 3	17	5	5	5	45
Информационный объект 4	5	3	4		12
Информационный объект 5	11	1		3	15
Информационный объект 6	7	5	2	2	16
Информационный объект 7	2	5		1	13

**Файлы**

MS Visio (msv)	22	11	4	6	43
Документ MS Word (doc, doc ...)	17	10	7	5	42
Сводная таблица (xls)	17	5	5	5	45
Растровое изоб. в формате P...	5	3	4		12
Растровое изоб. в формате GI...	11	1		3	15
Документ MS Word (doc, doc ...)	7	5	2	2	16
Сводная таблица (xls)	2	5		1	13

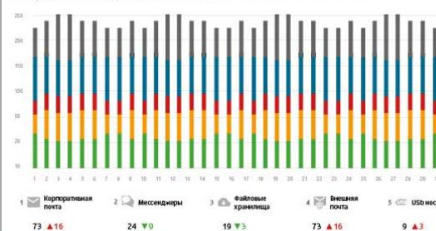
**Сводный отчет по инцидентам** за период 01.07.15 - 01.08.15

Общие показатели

- 2768 ↓ 172 зарегистрированных событий
- 2171 ↑ 71 обработанных событий
- 24 ↑ 2 на них инциденты
- 19 ↑ 1 закрыты инциденты

Профиль нарушений по инцидентам

Распределение инцидентов по каналам связи



По информационным объектам

73 ↑ 16	Тендерная документация	73 ↑ 16
24 ↑ 9	Финансовые отчеты	24
19 ↑ 3	Секретные документы	19 ↑ 3
73 ↑ 16	Документы особого контроля, и высшей секретности	73 ↑ 16
9 ↓ 3	Акционерные отчеты	9 ↓ 3

## 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?..





Узнайте больше про Solar Dozor!

Контакты ДиалогНаука:

[marketing@DialogNauka.ru](mailto:marketing@DialogNauka.ru)

8 (495) 980-67-76

Василий Лукиных

Менеджер по развитию бизнеса

Solar Security

[V.Lukinykh@solarsecurity.ru](mailto:V.Lukinykh@solarsecurity.ru)

+7 915 303 00 08