



КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ

# КАК ПЕРЕЙТИ ОТ КОНТРОЛЯ К УПРАВЛЕНИЮ КОРПОРАТИВНЫМИ ДАННЫМИ

Новые кейсы информационной  
безопасности

Светлана Марьясова  
*Региональный представитель, InfoWatch*



# Усложняются модели угроз



Электронная почта

Руководители

Системные администраторы

Бывшие сотрудники

**Сеть**

Мобильные устройства

(браузер, облако)

Кража или потеря оборудования

Бумажные документы

Съёмные носители (USB и т.д.)

**Мгновенные сообщения**

(текст, голос, видео)

Хакеры и другие внешние злоумышленники

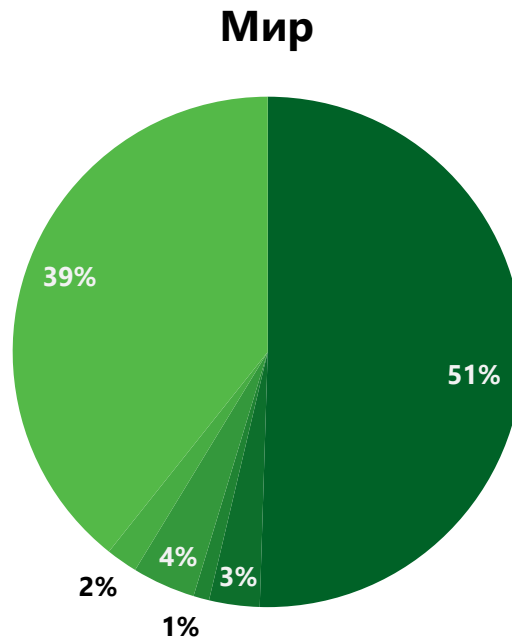
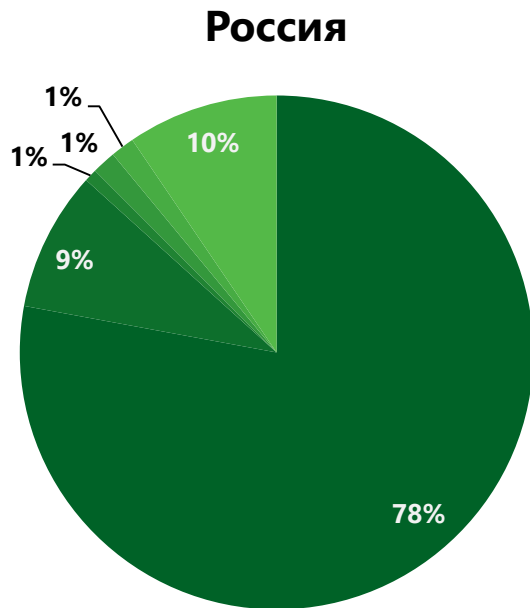
**Рядовые сотрудники**

Подрядчики

Привилегированные пользователи

# Усложняются модели угроз

Виновники утечек, 2018 год:

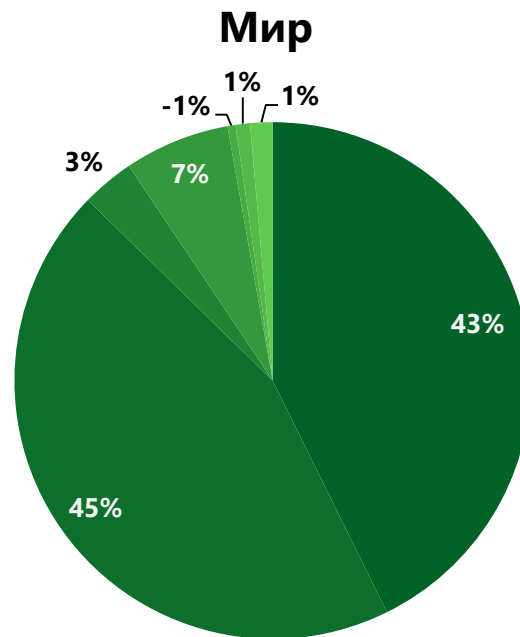
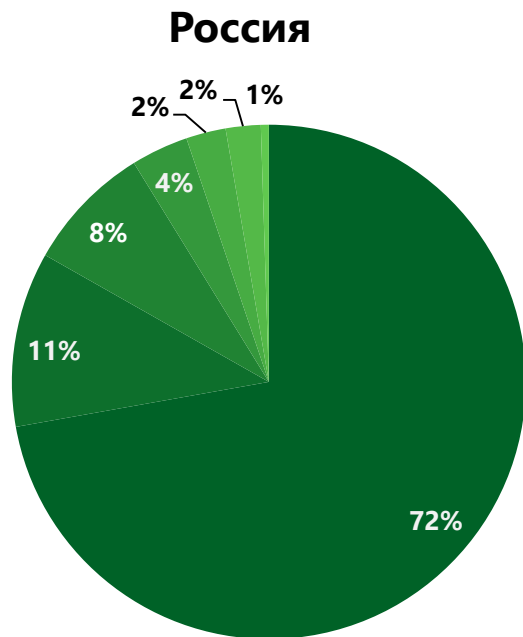


- Рядовые сотрудники
- Руководители
- Системные администраторы
- Подрядчики
- Бывшие сотрудники
- Хакеры и другие внешние злоумышленники

данные аналитического центра InfoWatch

# Усложняются модели угроз

Каналы утечек, 2018 год:



- Сеть (браузер, облако)
- Бумажные документы
- Электронная почта
- Мгновенные сообщения (текст, голос, видео)
- Кража или потеря оборудования
- Съёмные носители (USB и т.д.)
- Мобильные устройства

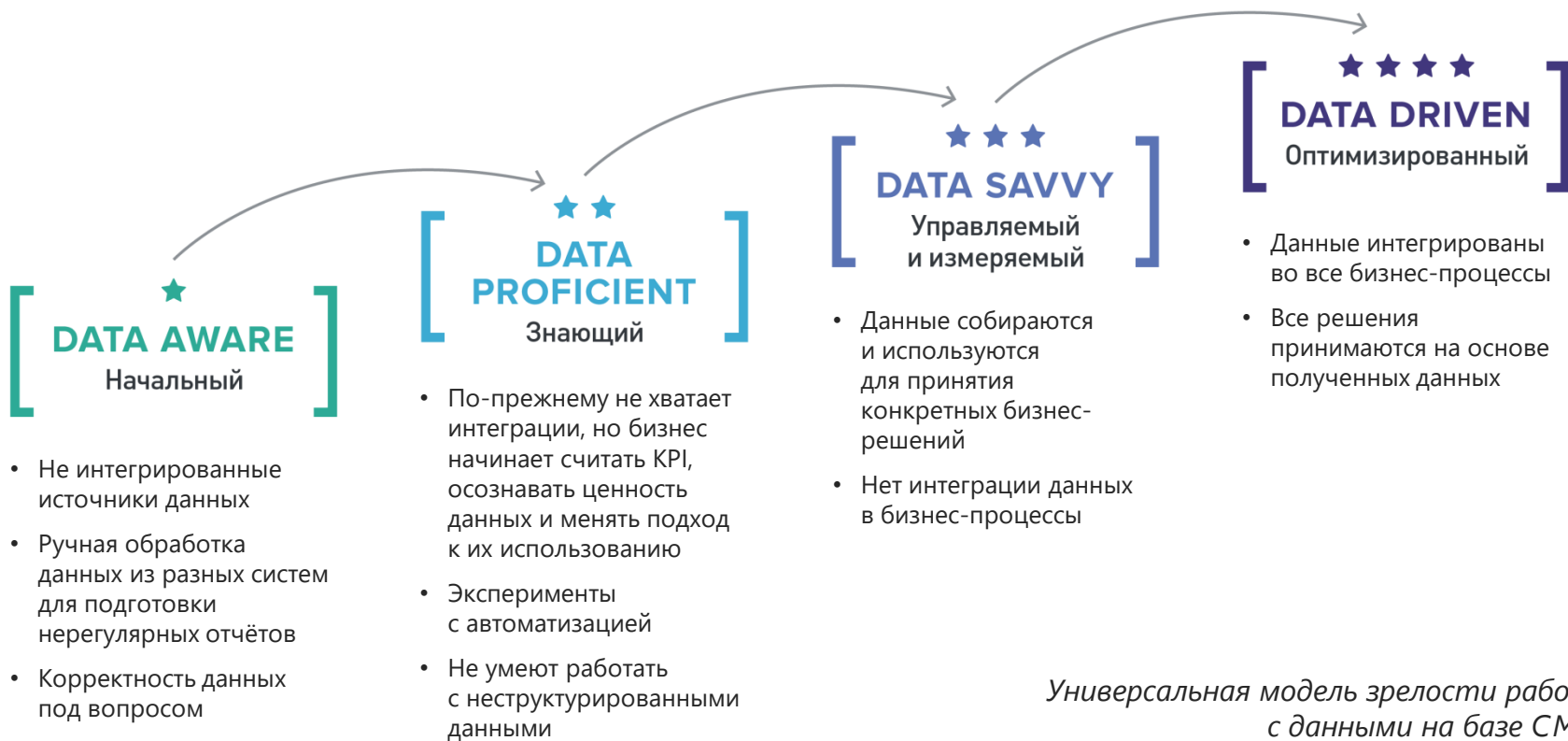
данные аналитического центра InfoWatch

## Безопасность от контроля переходит к управлению процессами:

- ✓ Управление рисками
- ✓ Работа с огромным массивом данных
- ✓ Анализ информационных потоков

- ✓ Второе рождение DLP-систем
- ✓ Эра визуализации
- ✓ ИБ, ЭБ и СБ взаимодействуют по DLP

# Работать с данными можно по-разному



# Чем отличается эффективная DLP-система от не очень эффективной?



Обработывает **миллионы событий**  
**в день, показывает только**  
**значимые** инциденты

Собирает **ограниченный набор**  
**данных, делает много ошибок**  
первого и второго рода



Запатентованные технологии лингвистического анализа:

- Определение категорий (тематики) на основании найденных терминов
- База контентной фильтрации (БКФ)
- Морфологический анализ более чем 35 языков
- Детектирование опечаток, замен и транслитерации
- Производительность решения позволяет анализировать до 2-х терабайт почтового трафика в день


Уникальные интеграционные решения с ведущими системами (SAP, SIEM, Cisco USM Adapter, Microlap EtherSensor и др.)

Реализованная в **InfoWatch Traffic Monitor** возможность точечной блокировки обеспечивает стабильность работы системы без прерывания бизнес-процессов.



## Специалист ИБ анализирует данные DLP-системы для проверки своих гипотез:

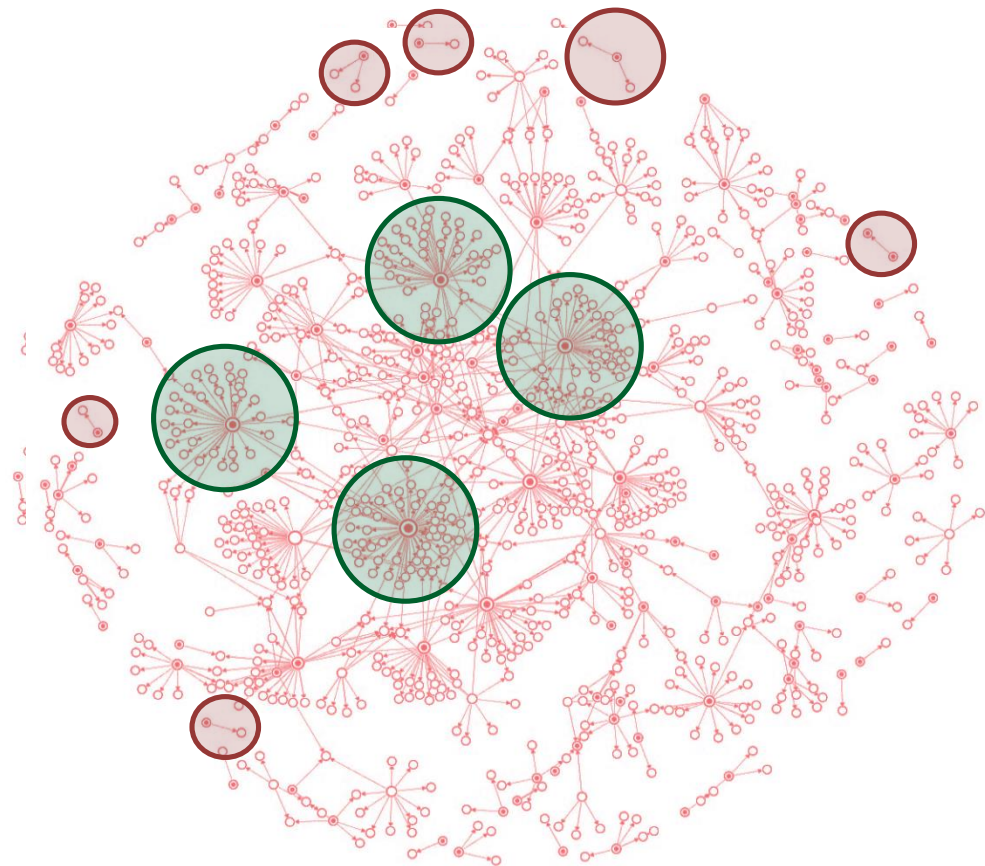
- Определить или сузить круг причастных к инциденту
- Собрать информацию о конкретном сотруднике и круге его общения
- Определить пути распространения информации
- Найти аномалии в поведении, коммуникациях
- Оценить актуальность политик ИБ
- Посмотреть сводные данные по компании

- 
- The diagram features a sailboat on the surface of the water, representing the visible part of an incident. Below the waterline, an iceberg is shown, representing hidden information. The iceberg is divided into five horizontal layers, each with a numbered circle and a corresponding text label. The layers are: 1. Детали взаимодействия (Details of interaction), 2. Сложившиеся процессы (Established processes), 3. Исторические данные и статистика (Historical data and statistics), 4. Неочевидные взаимосвязи (Unobvious connections), and 5. Скрытые инсайты (Hidden insights).
- 1 Детали взаимодействия
  - 2 Сложившиеся процессы
  - 3 Исторические данные и статистика
  - 4 Неочевидные взаимосвязи
  - 5 Скрытые инсайты



Инструмент визуального анализа данных, который повышает КПД и расширяет область применения DLP-системы InfoWatch Traffic Monitor

Показывает историю, которая кроется за миллионами сухих фактов, убирает шум и **подсвечивает полезную информацию**



- Зачем нужен граф связей на 10 тысяч узлов
- Можно ли извлечь из этого множества точек что-то полезное
- Даже в этом хаосе можно выявить аномалии
- Фильтрами можно убрать все «лишнее»
- «Топ нарушителей» показывает неправильные политики
- Реальные нарушения лежат на периферии

А ещё...



InfoWatch Vision даёт возможность взять под контроль «серую зону»

Проверить  
соответствие  
политик ИБ текущим  
бизнес-процессам

Выявить скрытые  
закономерности  
и неожиданные  
факты

Обнаружить  
неочевидные связи  
между отдельными  
детальми  
и восстановить  
цепь событий

# Добраться до сути за пару кликов



Локализовать проблему и сузить круг подозреваемых



Выявить аномалии в предположительно легитимном трафике



Определить круг общения и выявить подозрительные связи сотрудника



Выяснить маршрут распространения информации в компании



Накопить информацию в досье для дальнейшего мониторинга и анализа



Сформировать профиль обращения сотрудника с информацией



Актуализировать настройки InfoWatch Traffic Monitor для выявления возможных угроз



Получить сводную статистику по компании, в том числе при использовании нескольких систем InfoWatch Traffic Monitor

## InfoWatch Vision помогает применить DLP-систему для НОВОГО ПЛАСТА ЗАДАЧ

Обнаружить проблемы взаимодействия между подразделениями

Составить полную картину взаимодействия сотрудника для оценки 360°

Выявить узкое место в коммуникациях и центры экспертизы

Восстановить разорванные связи при увольнении сотрудника

Учесть неформальные связи при принятии управленческих решений

Выявить внутренние конфликты и нарушения правил коммуникаций



Специалист ИБ включает **InfoWatch Person Monitor**, когда в фокусе расследования оказывается конкретный сотрудник и необходимо:

- Восстановить полную картину событий
- Собрать доказательную базу при расследовании
- Установить причины инцидента

Собрать полную информацию о действиях пользователя и создать недостающую связь между **учетной записью** и **реальным сотрудником**:

- Запись скриншотов и видео с экрана, изображения с веб-камеры, звук с микрофона и динамиков
- Входящие и исходящие сообщения электронной почты, вложенные файлы
- Мониторинг коммуникаций в мессенджерах Lync, Skype, Teams, Viber, Telegram, WhatsApp, Bitrix24 и т.д.
- Посещаемые сайты и интернет-запросы, передача файлов через файлообменники, веб-почту и чаты
- Статистика использования приложений и мониторинг вводимого текста
- Операции с документами: удаление, печать, копирование на внешние носители и в облако
- Факт присутствия на рабочем месте и в офисе, время, проведенное за компьютером
- Геолокация мобильных устройств и ноутбуков на платформах Android, Windows 10



- Анализ операционной эффективности;
- Прогнозирование рисков;
- Выявление потенциальных признаков подготовки к инциденту;
- Предотвращение нарушения;
- Управление рисками



Полезная информация на нашем стенде:

- Чек-лист для АСУТП
- Схема процесса-реагирования на инциденты
- Модель зрелости работы с данными

Уже совсем скоро:

- **BIS Summit 2019**

24 сентября, Москва, Конгресс-парк  
гостиницы «Украина»

- Аналитический отчет  
за первое полугодие  
2019 года по утечкам

Будем на связи:



Подпишитесь на рассылку

#CODEIB

**Спасибо  
за внимание!**



**Светлана Марьясова**  
*Региональный представитель, InfoWatch*

+7 (950) 415-32-00

[Svetlana.Maryasova@infowatch.ru](mailto:Svetlana.Maryasova@infowatch.ru)



**КОД  
ИНФОРМАЦИОННОЙ  
БЕЗОПАСНОСТИ**