КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ

Новый информационный ландшафт — 2021

Как защищать конфиденциальные данные в изменившихся условиях

Светлана Марьясова

Менеджер по работе с клиентами и партнёрами в СФО, InfoWatch

УТЕЧЕК СТАЛО МЕНЬШЕ!?

ВСЁ НАМНОГО ХУЖЕ. МЫ ТЕПЕРЬ НЕ ЗНАЕМ О НИХ!

INFOWATCH®

Объём пользовательских данных, скомпрометированных в результате утечек*

1–9.2019

10,1 млрд

1–9.2020

9,93 млрд

*Глобальное исследование утечек информации в 2020 (январь — сентябрь)

Откуда ждать сложностей?

INFOWATCH®

Технологии

→ **Новые каналы коммуникации** (мессенджеры и трекеры задач замещают почту)

→ **Новый информационный ландшафт, распространение гибридных рабочих систем**

Люди

→ **Новая модель коммуникации** (менее формальная, более короткие сообщения)

Сложнее контролировать информационные потоки.

INFOWATCH®

ЧТО ДЕЛАТЬ?

→ Технологии

Основная задача — восстановить контроль над информационной средой и инфраструктурой с учётом их изменений

Что будет новой нормой?

INFOWATCH®

Контроль работы непосредственно в бизнес-системах

Проверенная возможность держать данные под контролем даже в случае дистанционного рабочего места

Применение предиктивной аналитики InfoWatch Prediction

Потому что ручной контроль неэффективен

Визуализация информационных потоков InfoWatch Vision

Пора заглянуть в «серую зону»

Цель: восстановить контроль над инфраструктурой с учётом её изменений.

Как восстановить контроль над инфраструктурой

Тогда

- Контроль рабочих станций в периметре

Сейчас

- Среда стала разнообразнее, значит, и контроль должен стать более гибким и разнообразным →

Контроль достигается с помощью интеграций

→ С Office 365, Exchange Online, MFlash

→ WorksPad

InfoWatch Traffic Monitor 7.1

DLP-система с технологиями машинного обучения на борту

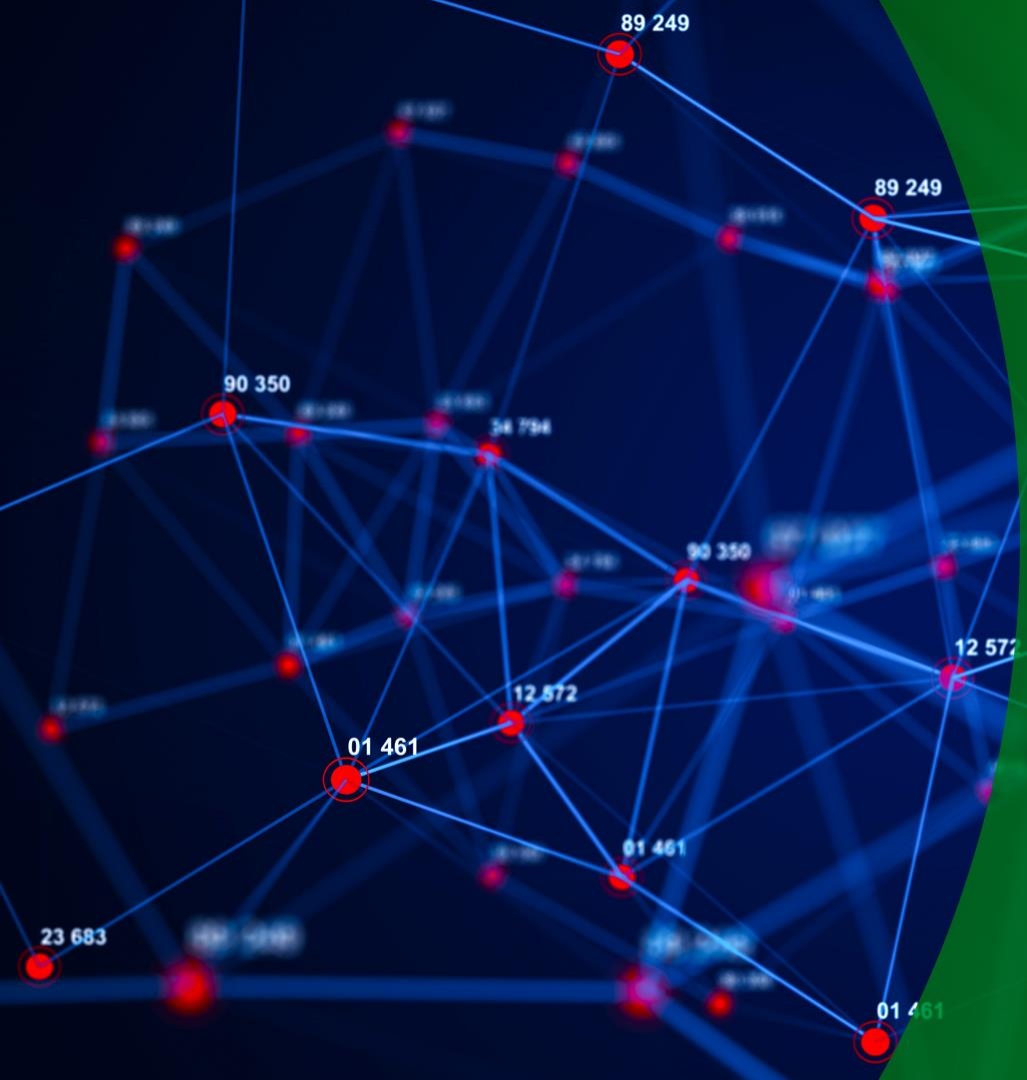
Контролирует не только основные каналы, но и самые «проблемные» —

Мобильные телефоны

Соцсети

Облачные сервисы

Проприетарные системы

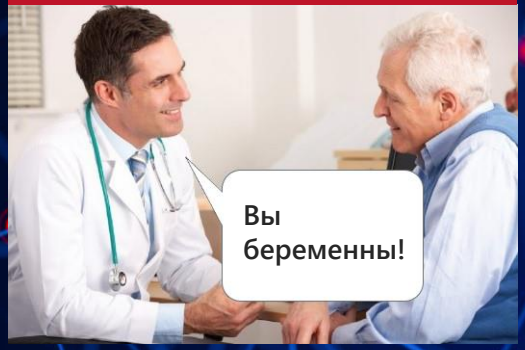


INFOWATCH®

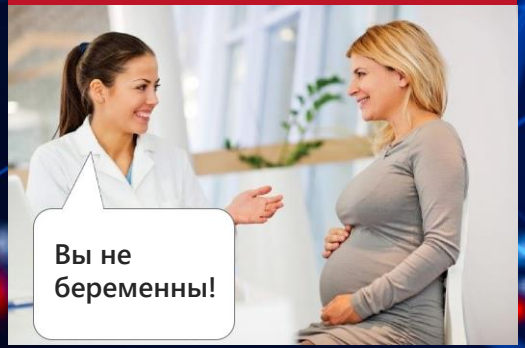
КОНТЕНТНЫЙ АНАЛИЗ

Почему сейчас это особенно важно?

Ошибка I-го типа: Ложноположительная



Ошибка II-го типа: Ложноотрицательная



Контентный анализ

Точность контентного анализа — критерий качества работы DLP-системы.

- → Не пропустить конфиденциальную информацию
- → Минимизировать ложные срабатывания

InfoWatch Traffic Monitor 7.1

DLP-система с технологиями машинного обучения на борту

INFOWATCH®

Точность контентного анализа

Выше эффективность

Минимум ложных срабатываний

28 патентов на контент-анализ

с **2006** применяем методы машинного обучения

Вы сможете защищать данные в условиях «постковидной эры».

А что нового?

INFOWATCH®

1

Мы видим:

Скорость изменения рабочих процессов кратно возросла

2

Значит:

Должна вырасти и скорость адаптации систем безопасности

3

Наш ответ:

Система автоматизации настройки DLP

А что нового? Как работает автоматизация

INFOWATCH®

1

Анализирует архив данных

Собирает документы и раскладывает их по «стопкам» (кластерам)

2

Помогает проверить качество кластера

Подбирает документы для проверки того, что в «стопку» попали однотипные документы

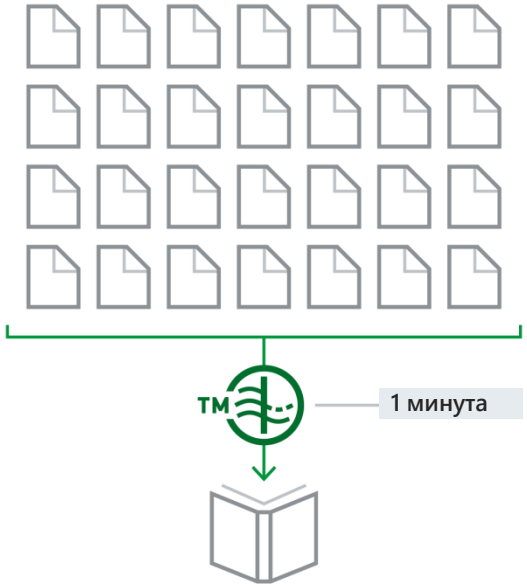
3

Готовит настройки для каждой «стопки»

Автоматически генерируется профиль для выявления документов подобным тем, что в «стопке»

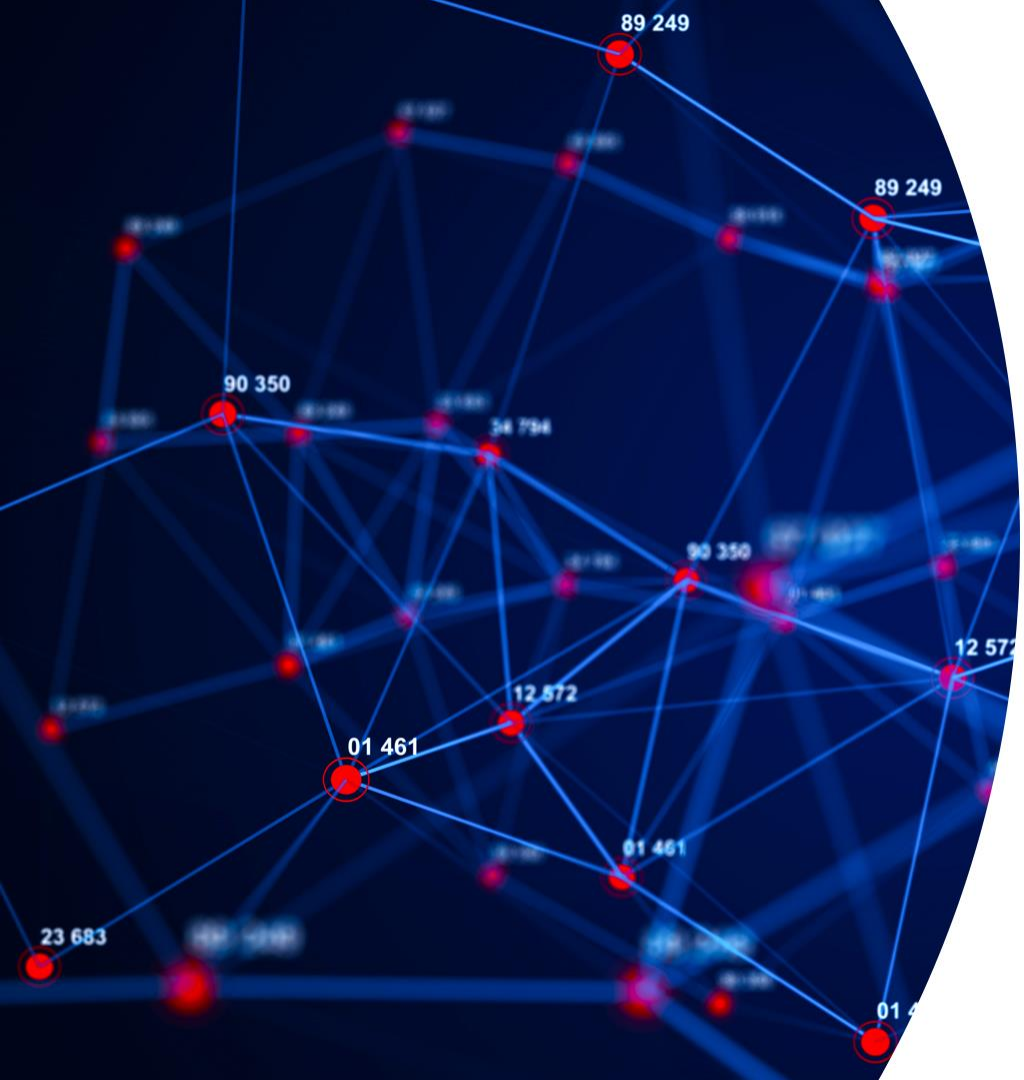
И это только первый шаг...

Технология, позволяющая научить DLP-систему определять любую новую категорию информации.



Машинное обучение, метод опорных векторов

- → Без специфических знаний лингвиста
- → Без изучения документов, без предварительной подготовки коллекции документов
- → Дополнительное обучение
- → Корректировка ЛПС



Автоматизация DLP: преимущества

→ **Не нужно просить у владельцев документов образцы данных для защиты**

Система сама найдёт их в архиве

→ **Не нужно разбираться в лингвистике**

Система сама подберёт настройки

→ **Это быстро**

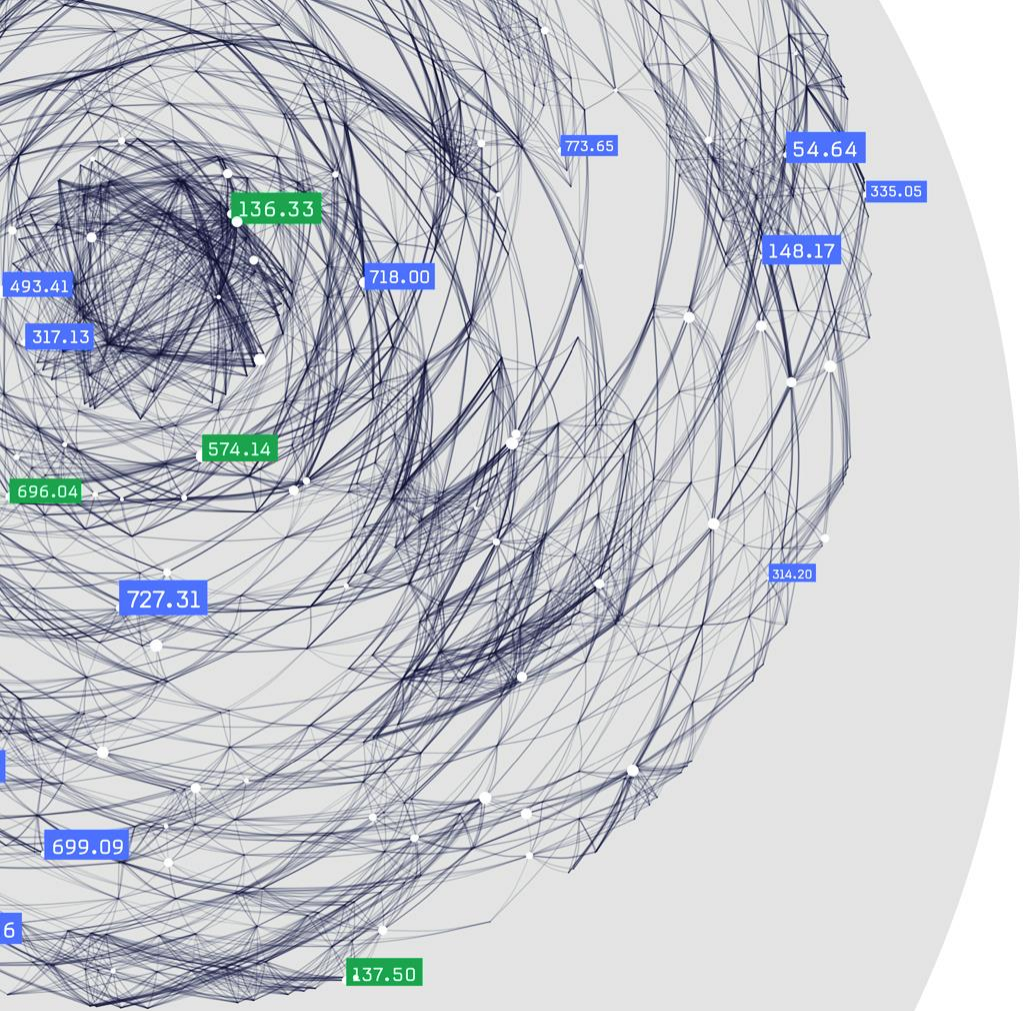
Минуты и часы вместо обычных недель и месяцев на настройку

INFOWATCH®

ЧТО ДЕЛАТЬ?

→ Люди

Поможет аналитика данных DLP

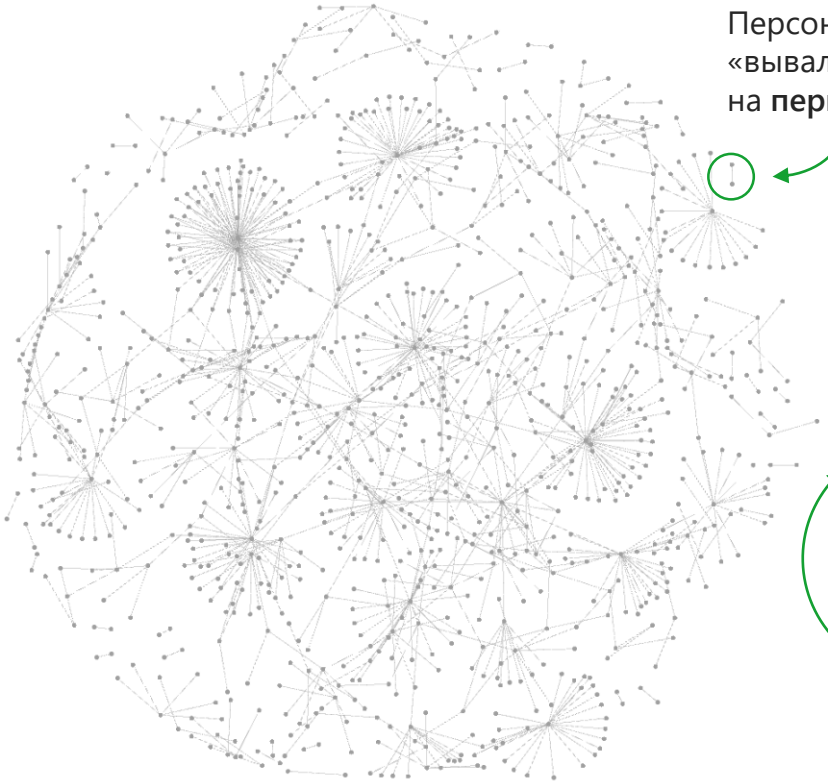


Современные технологии InfoWatch для ИБ

→ **Профилактика отнимает большое количество человеческих ресурсов.** Сейчас на помощь пришла автоматизация

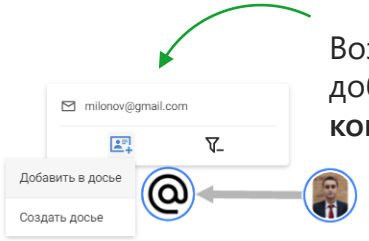
→ **Не только визуальная, но и ПРЕДИКТИВНАЯ аналитика** становятся новой нормой работы служб ИБ

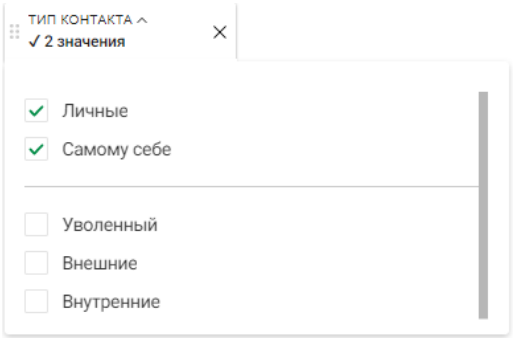
Отслеживание персональных коммуникаций в InfoWatch Vision



Персональные коммуникации «вываливаются» на **периферию** графа

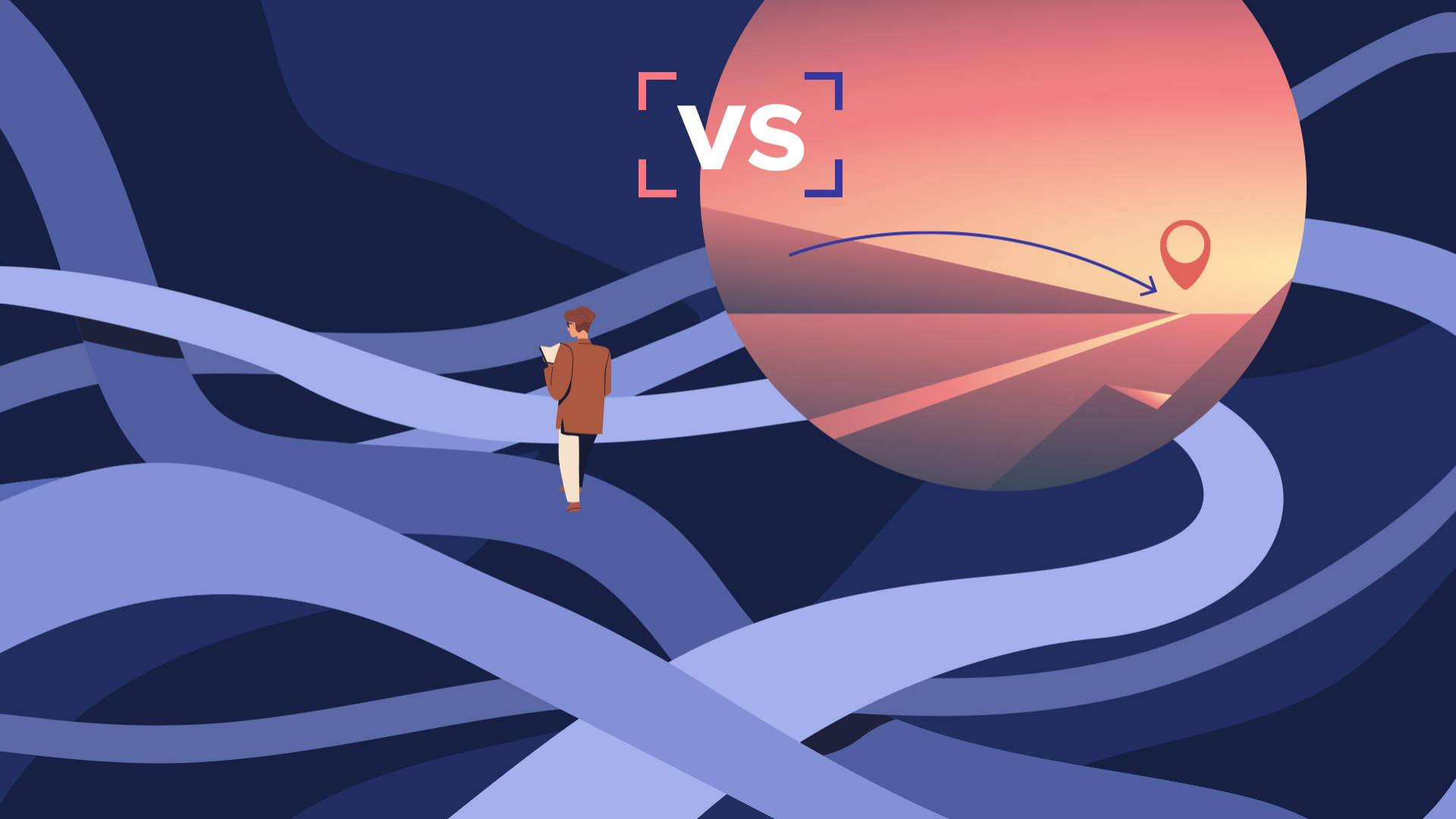
Возможность добавить **личный контакт** на графе





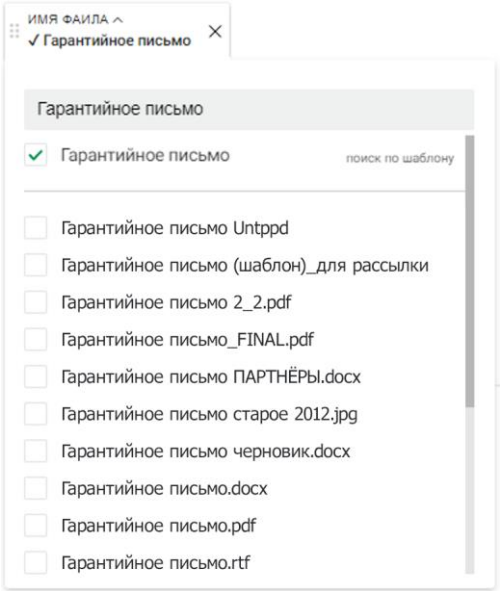
Фильтр позволяет отобрать все события с личными контактами

\+ Фильтр **«Уволенные»** позволяет отобразить переписку с бывшими коллегами

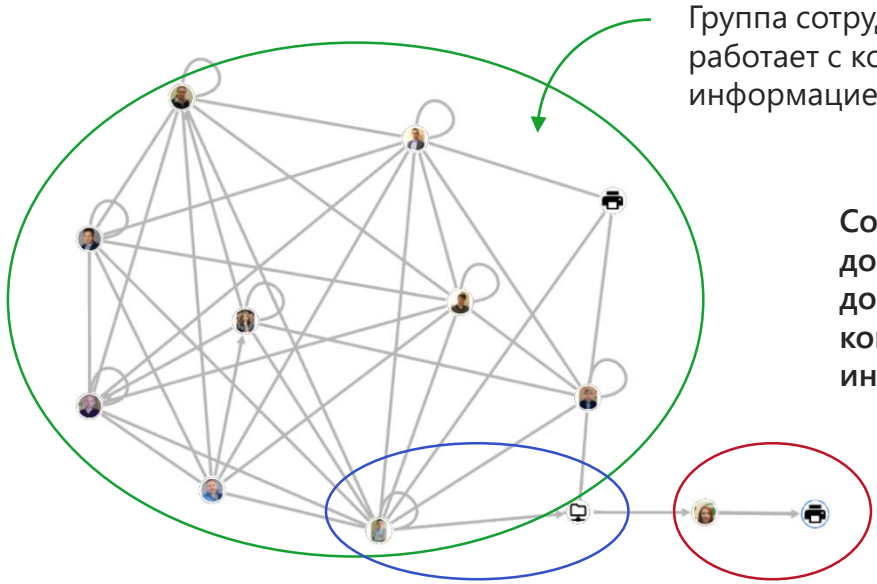

VS

Как провести расследование за 10 минут, а не за несколько часов?

1. **Поиск по общей части в имени файла**



2. **Граф связей перемещения информации в компании**



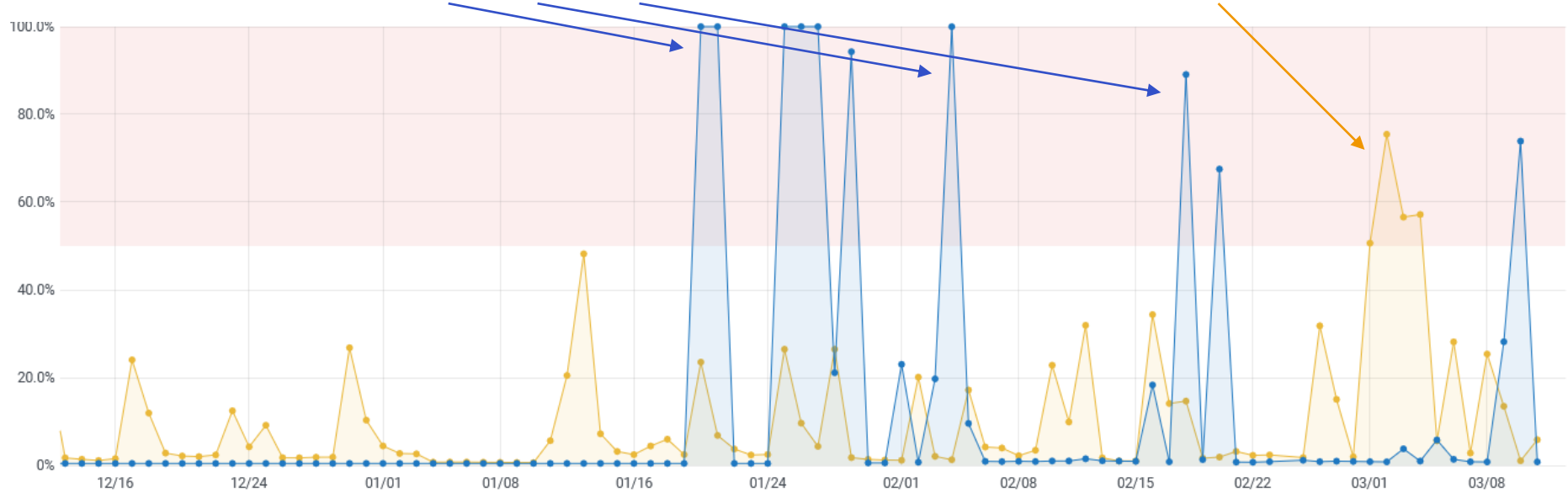
3. **Теперь вы знаете!**

Предиктивная аналитика

Вместо констатации фактов утечек и устранения последствий — прогнозирование, профилактика и предотвращение нарушений.

Копирование файлов
на внешние носители

Негативные отзывы
о компании или начальстве



Итог

INFOWATCH®

1

Настоящая гонка за эффективностью. Даже для тех, кто раньше внедрял технологии ИБ только «для галочки»

→ Продуманные интеграции DLP с инфраструктурами

→ Автоматизация для повышения эффективности работы

2

Придётся оценивать риски и демонстрировать умение и возможность мгновенно реагировать на изменения

→ Качественно иные результаты, которые даёт визуальная и предиктивная аналитика, становятся новым стандартом / нормой в работе ИБ-служб

И напоследок: сертификация по новым правилам

INFOWATCH®

Сертифицированы ФСТЭК России

InfoWatch Traffic Monitor

InfoWatch Person Monitor

- → Сертификат соответствия **№ 4340** на **InfoWatch Traffic Monitor: версия 7**
  16 декабря 2020
- → Сертификат соответствия **№ 4206** на **InfoWatch Person Monitor:** требования РД НДВ (4) и ТУ
  23 января 2020
- → Разработка **в соответствии с методологией SDL**

Чтобы ваша DLP не стала той самой «дырой в безопасности».

#CODEIB

СПАСИБО ЗА ВНИМАНИЕ!

ПРИГЛАШАЮ ПРОДОЛЖИТЬ РАЗГОВОР НА СТЕНДЕ INFOWATCH

Светлана Марьясова

Менеджер по работе с клиентами и партнёрами в СФО, InfoWatch

Svetlana.Maryasova@infowatch.com

Больше полезной информации:

/InfoWatchOut

/InfoWatch

/infowatchnews