INFOWATCH®

Новый информационный ландшафт 2021

Как защищать конфиденциальные данные в изменившихся условиях.

/InfoWatchOut /InfoWatch /infowatchnews

Утечек стало меньше!?

INFOWATCH®

Все намного хуже. Мы теперь не знаем о них!

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

ЧТО ДЕЛАТЬ?

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

Что будет новой нормой?

→ 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

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»

Автоматизация DLP

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

Автоматизация DLP: как работает

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

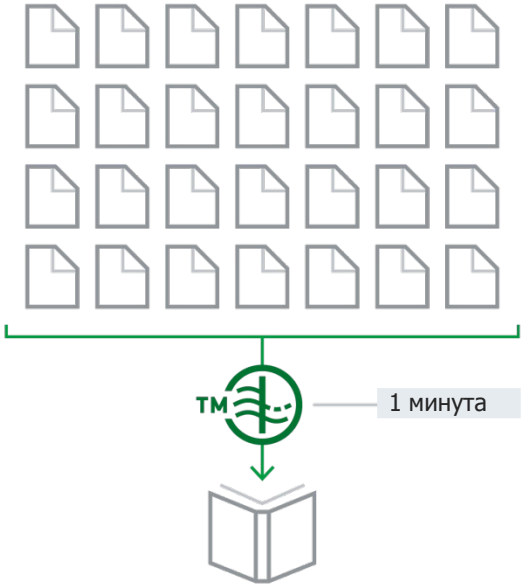
3

Готовит настройки для каждой «стопки»

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

Наш 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 их сама найдёт в архиве

- Не нужно разбираться в лингвистике

  Система подберёт настройки сама

- Это быстро

  Минуты и часы вместо обычных недель и месяцев на настройку

INFOWATCH®

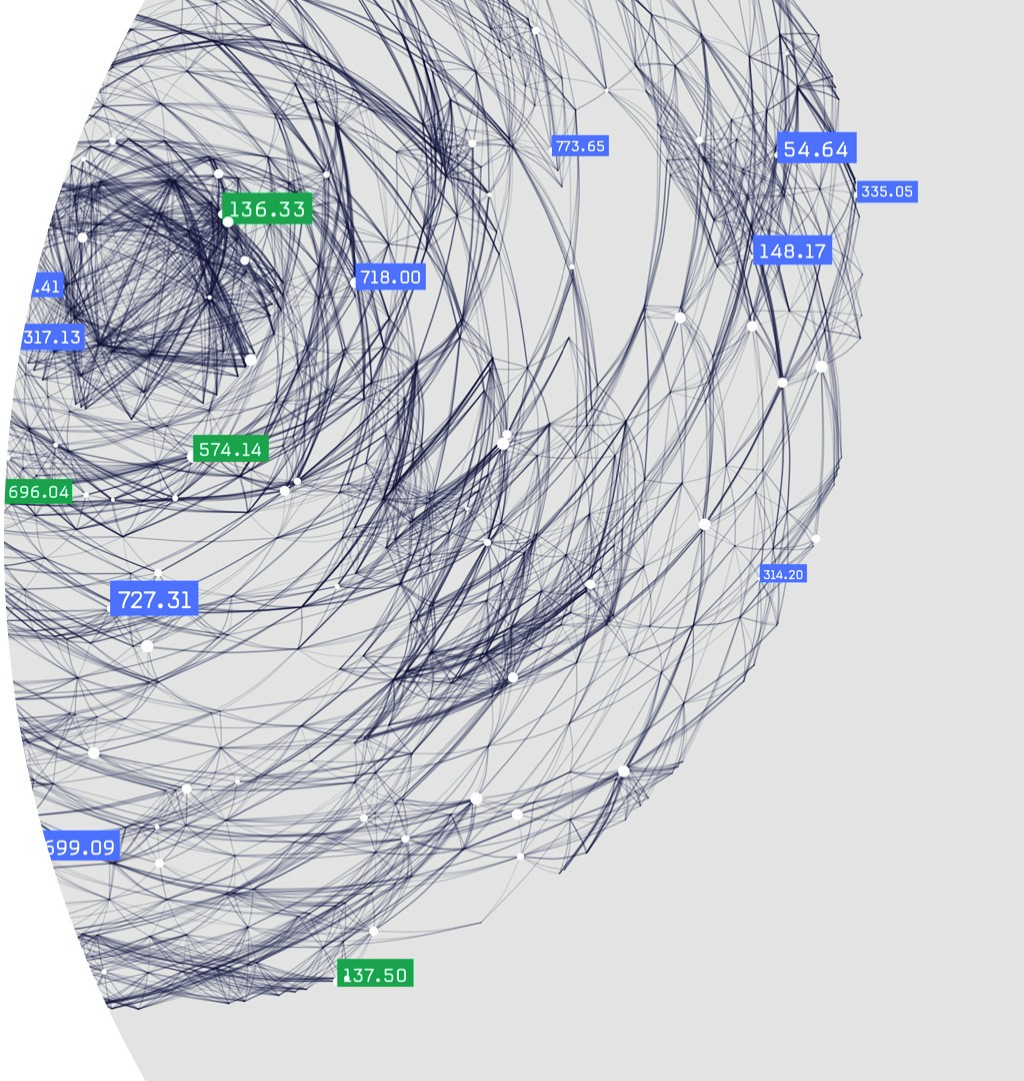
ЧТО ДЕЛАТЬ С ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ?

Поможет аналитика данных DLP

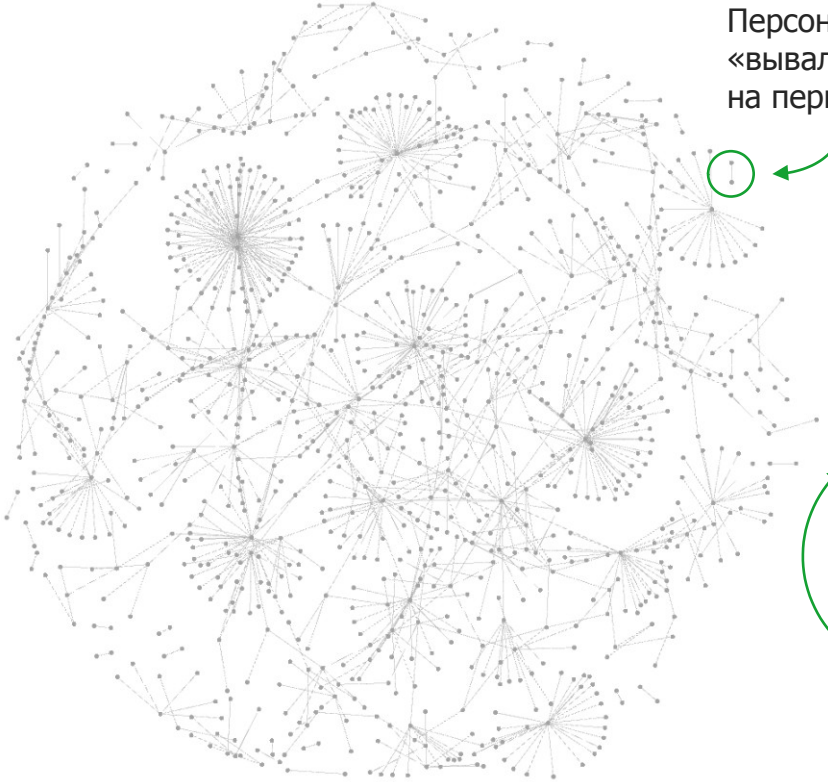
Современные технологии InfoWatch для ИБ

- Исторически так сложилось, что профилактика отнимает большое количество человеческих ресурсов. Сейчас на помощь пришла автоматизация

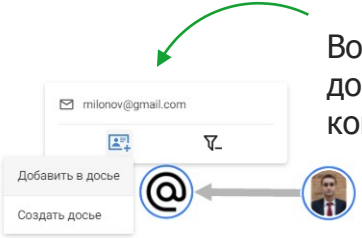
- Не только визуальная, но и ПРЕДИКТИВНАЯ аналитика становятся новой нормой работы служб ИБ



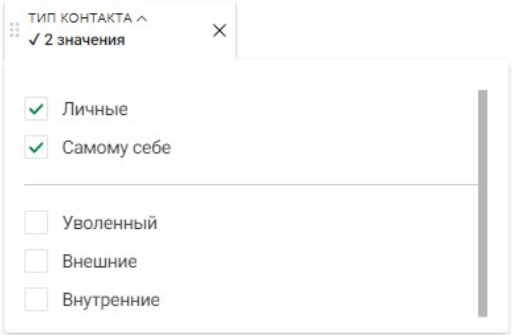
Отслеживание персональных коммуникаций в InfoWatch Vision



Персональные коммуникации «вываливаются» на периферию графа



Возможность добавить личный контакт на графе

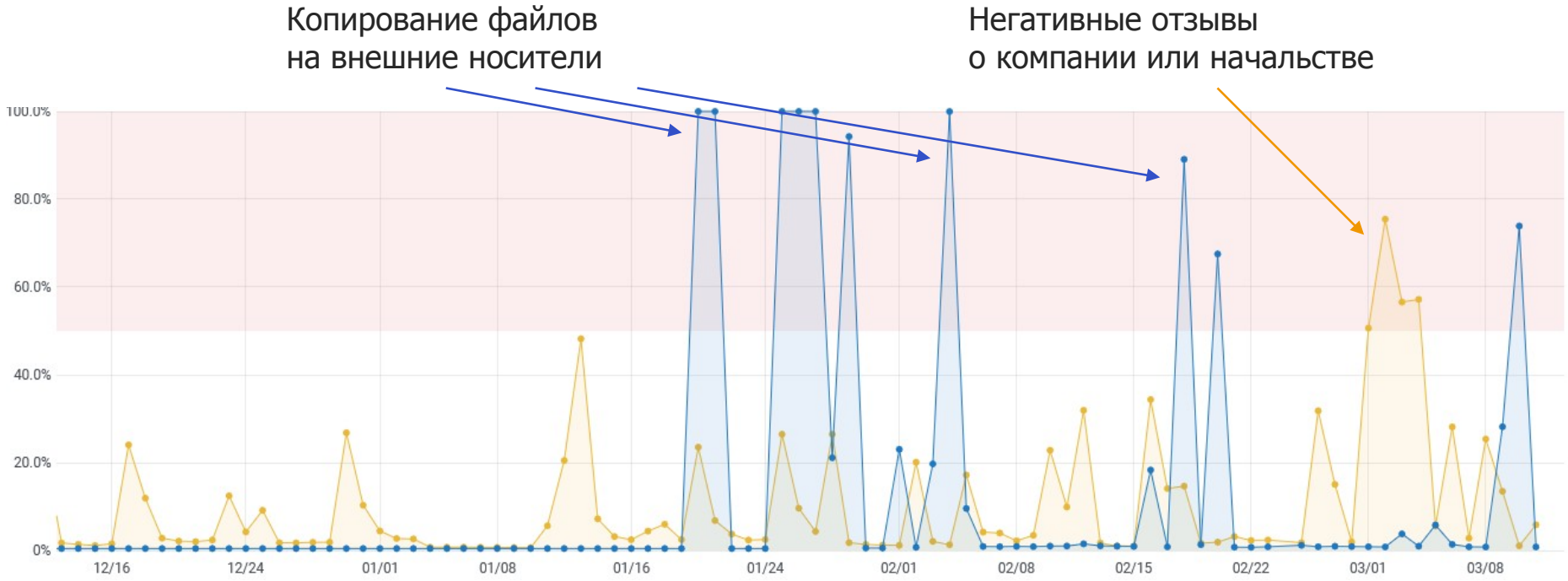


Фильтр позволяет отобрать все события с личными контактами

+ Фильтр «Уволенные» позволяет отобразить переписку с бывшими коллегами

Предиктивная аналитика

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



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 РФ

InfoWatch Traffic Monitor

InfoWatch Person Monitor

- Сертификат соответствия **№ 4340** на InfoWatch Traffic Monitor версия 7 (16.12.2020
- Сертификат соответствия **№ 4206** на InfoWatch Person Monitor: требования РД НДВ (4) и ТУ (23.01.2020)
- Разработка в соответствии с методологией SDL

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

INFOWATCH®

Больше полезной информации:

/InfoWatchOut

/InfoWatch

/infowatchnews