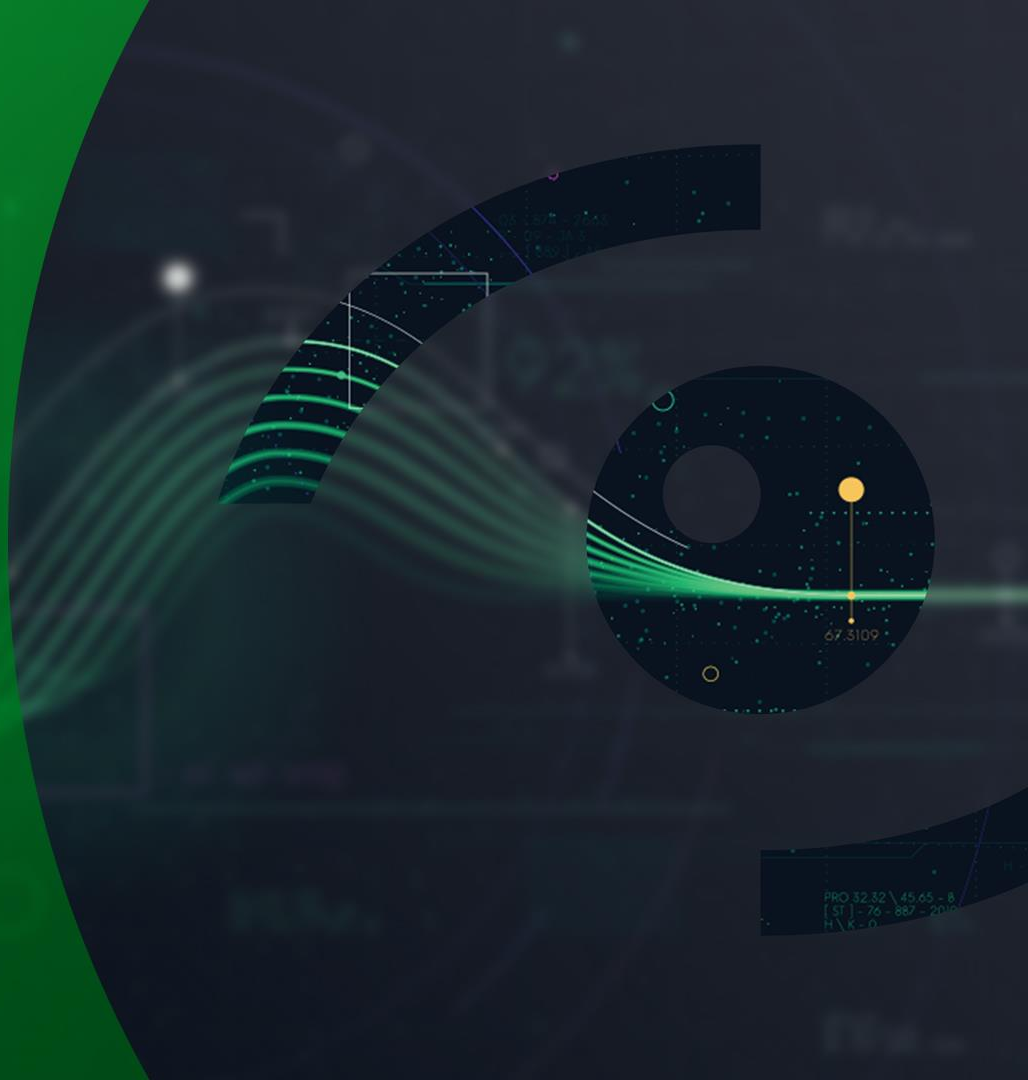
INFOWATCH®

СОВРЕМЕННЫЕ ПОДХОДЫ К СОХРАННОСТИ ИНФОРМАЦИИ

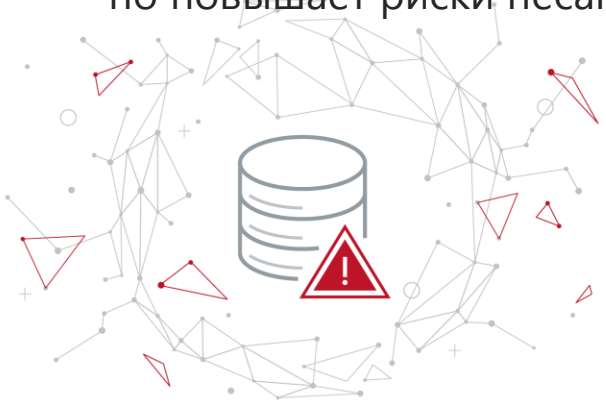
в постковидную эру



Изменения цифровой среды — новые вызовы

Цифровая трансформация

Увеличивает производительность и конкурентоспособность,
но повышает риски несанкционированного доступа к информации.



Ужесточение требований регуляторов

Постковидная эра

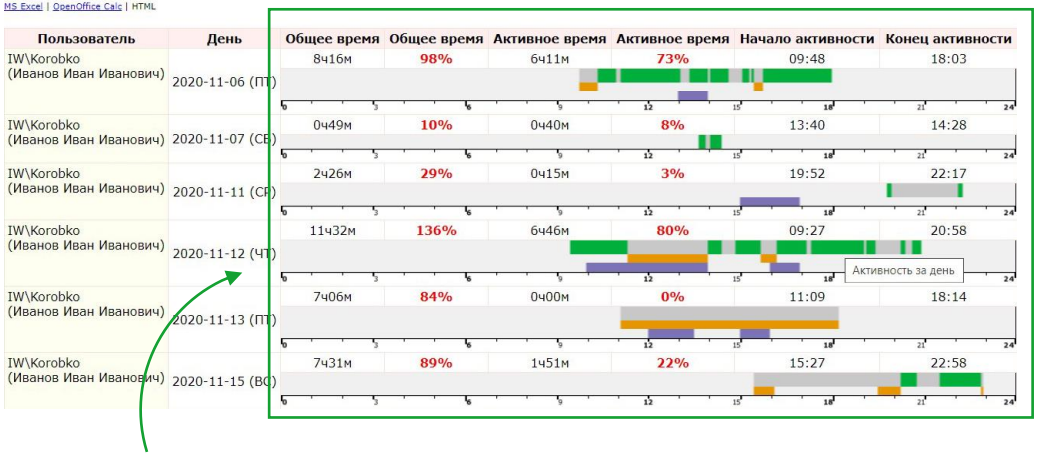
Показала, что периметр размыт, и усложнила задачу защиты корпоративных данных.

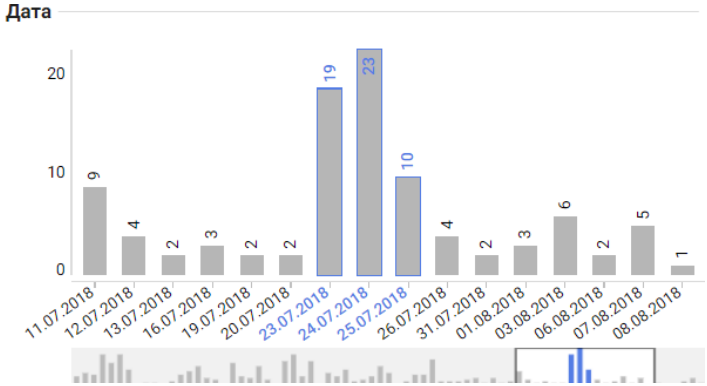
INFOWATCH®

ЧТО ДЕЛАТЬ?

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

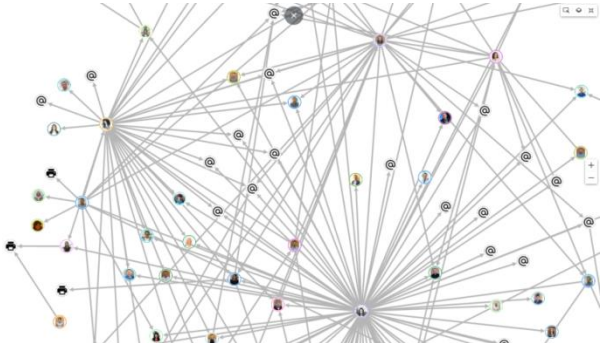
Как установить контроль над «серой зоной»



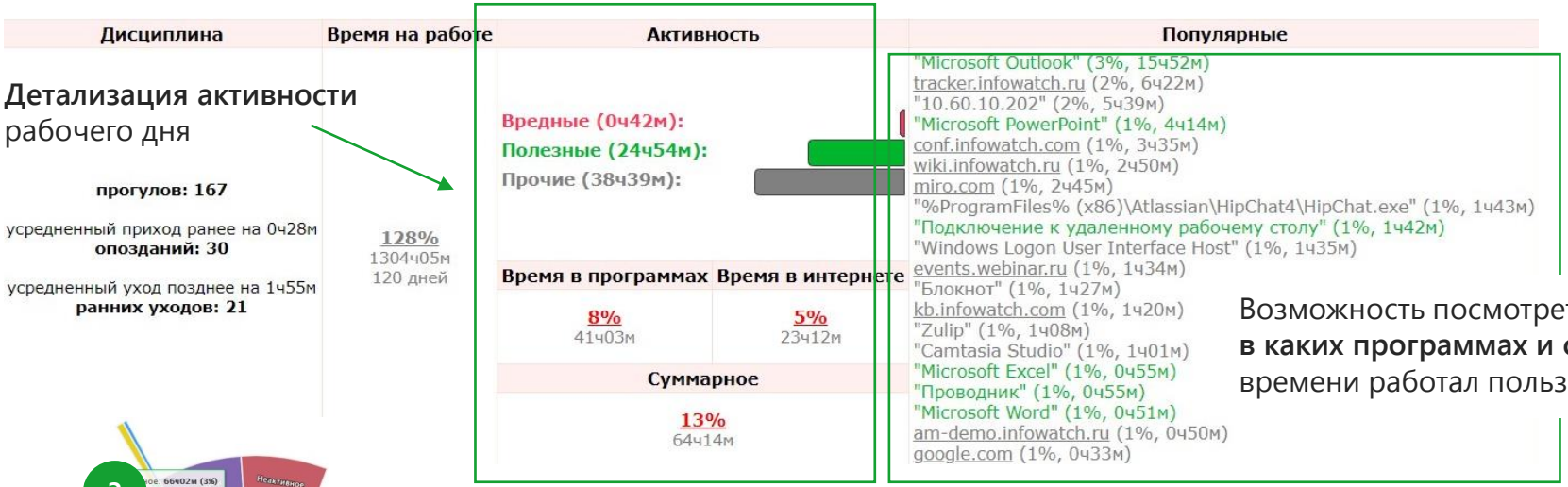


Полная картина рабочего дня сотрудника

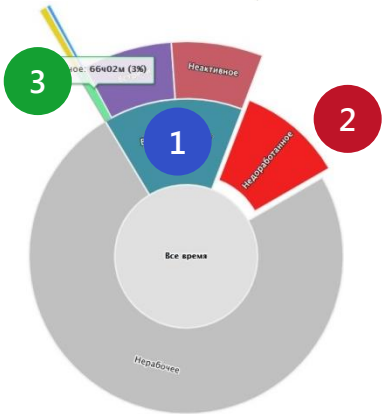
- → Выявление **аномальных всплесков** активности
- → Проверка **легитимности обмена** конфиденциальной информацией внутри организации
- → Обнаружение **подозрительных коммуникаций** между отделами и должностями
- → **Мгновенная проверка гипотез** с помощью Drill down



Оценка характера активности пользователя



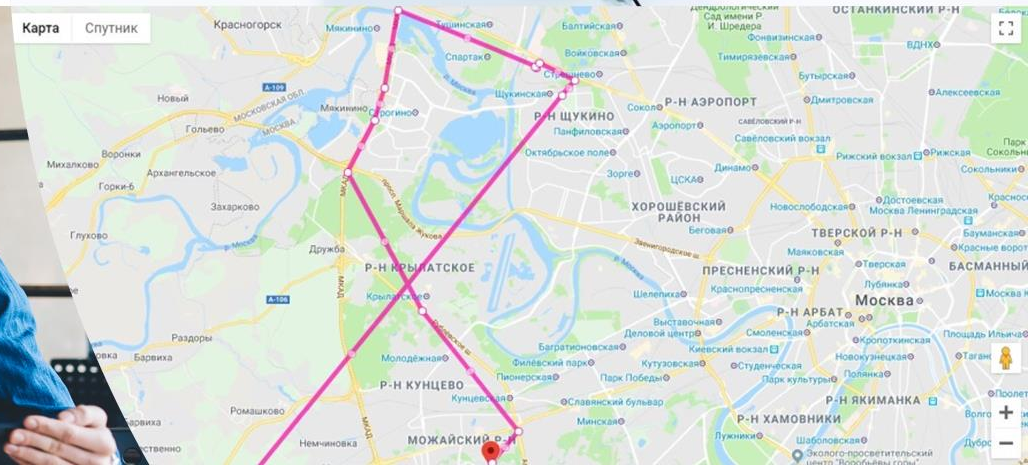
Возможность посмотреть, **в каких программах и сколько** времени работал пользователь



1. **Общее время** сотрудника (в часах) с момента первого «залогинивания» до последнего «разлогинивания»
2. **Сколько сотрудник переработал** за выбранный временной интервал
3. **Активное время работы** сотрудника
4. **Время на встречах** (из персональных календарей сотрудника)

Контроль конечных устройств

- → Возможность получения информации **с веб-камер на удалёнке**
- → Данных **из кейлоггера и геолокации**



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®

ЧТО ДЕЛАТЬ С ЧЕЛОВЕЧЕСКИМ ФАКТОРОМ?

Сотрудники в обход rdp копируют корпоративные данные локально на ноутбуки.

Саботаж со стороны сотрудников

INFOWATCH®

удаление из "сетевой диск/папка":

[2021-03-12 12:12:55] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Печать\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Лингвистика\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Графические файлы\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Выгрузки БД\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\OCR\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\БКФ\Энергетика\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\БКФ\Нарушение законодательства\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\БКФ\БКФ Азербайджан Банк\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\БКФ\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\Personal data\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\Medical records\
Medical Card.pdf
Release of health information.pdf

[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\IT\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\HR\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\Financial & legal\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\Constructor's documents\
Construction-Document-1.jpg
method-constructionmodel1.jpg

[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\INTNTL\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\DMM events\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Файлы\тест эталонок\
database.csv
database.xlsx

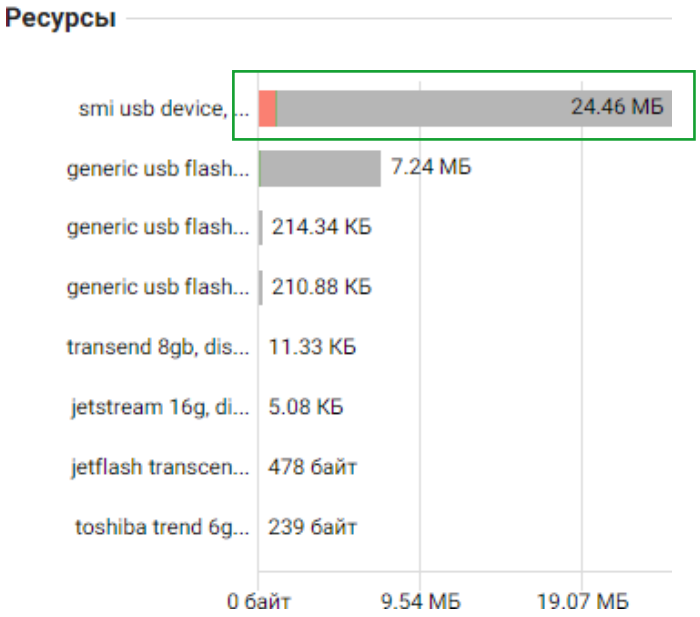
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Файлы\БД отпеч\
company_list.txt
stock_members_details.csv
stock_members_details_catch.xls

[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Файлы\Анкета\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Файлы\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\обучение\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Эталонные текстовые доки\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Формы\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Тестовая коллекция чертежей\
[2021-03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Текстовые шаблоны\
avascript:; -03-12 12:13:21] \\infowatch.ru\set\IWProducts\actual\Person_Monitor\8.67\Distr files\DEMO files\Новые объекты защиты\Текстовые объекты\

Один из вариантов саботажа — массовое удаление файлов с сетевых хранилищ.

Система **информирует об удалении** корпоративных данных.

Пример, когда только DLP не поможет



На виджете «Ресурсы» выявлен USB-накопитель, куда за 2 недели был скопирован большой объём информации.

Нарушение политик DLP не зафиксировано — документы копировались небольшими порциями и большая их часть не относилась к категорированной информации.

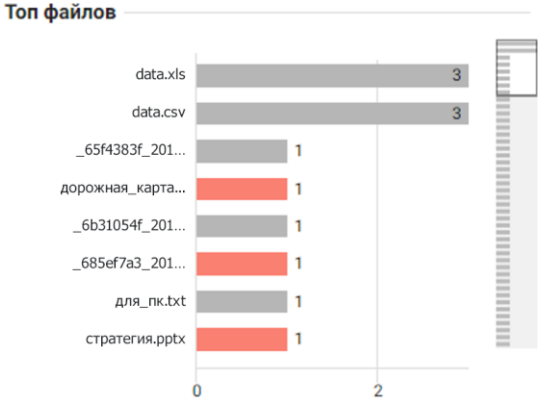
Пример, когда только DLP не поможет

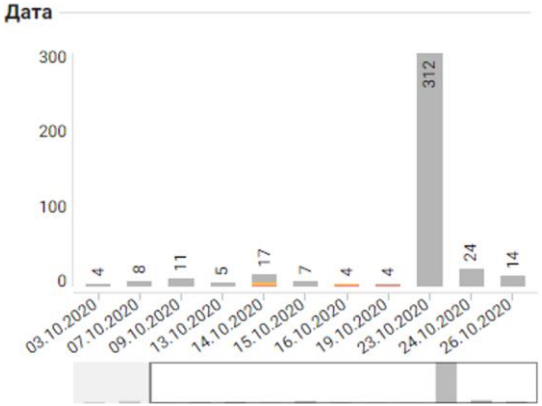
INFOWATCH®

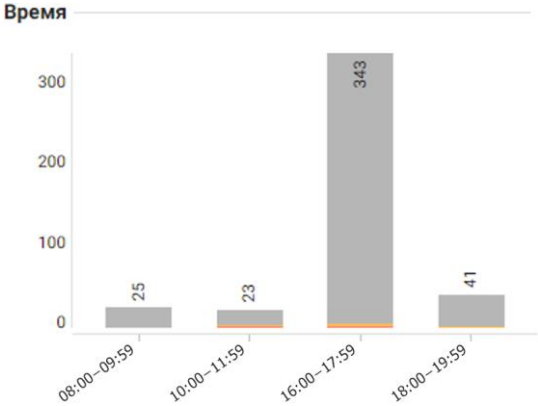
- → Устройство добавлено в условия фильтрации и по нему **построен отчёт**
- → **Анализ списка файлов** показал, что на USB-накопитель выведено большое количество рабочих документов сотрудника

- → На виджете **«Дата»** видно — сотрудник копировал документы в течение месяца, постепенно увеличивая их количество

- → На виджете **«Время»** видно — копирование производилось, в основном, в утренние и вечерние часы, чтобы не привлекать внимание

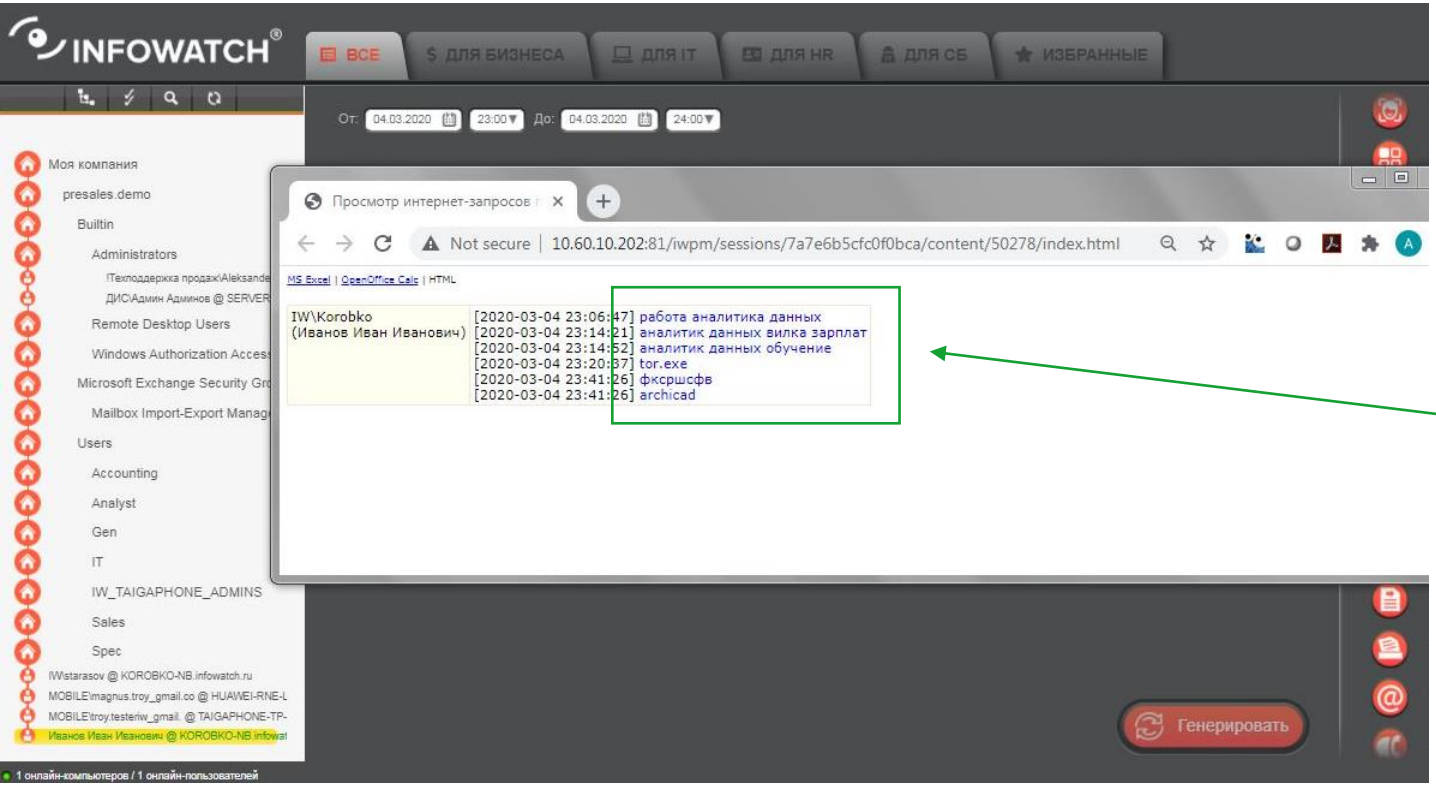






Флешка была вовремя изъята. В результате разъяснительной беседы сотрудник признался, что собирал портфолио и готовился к увольнению.

Как ещё можно понять, что сотрудник готовится к увольнению?



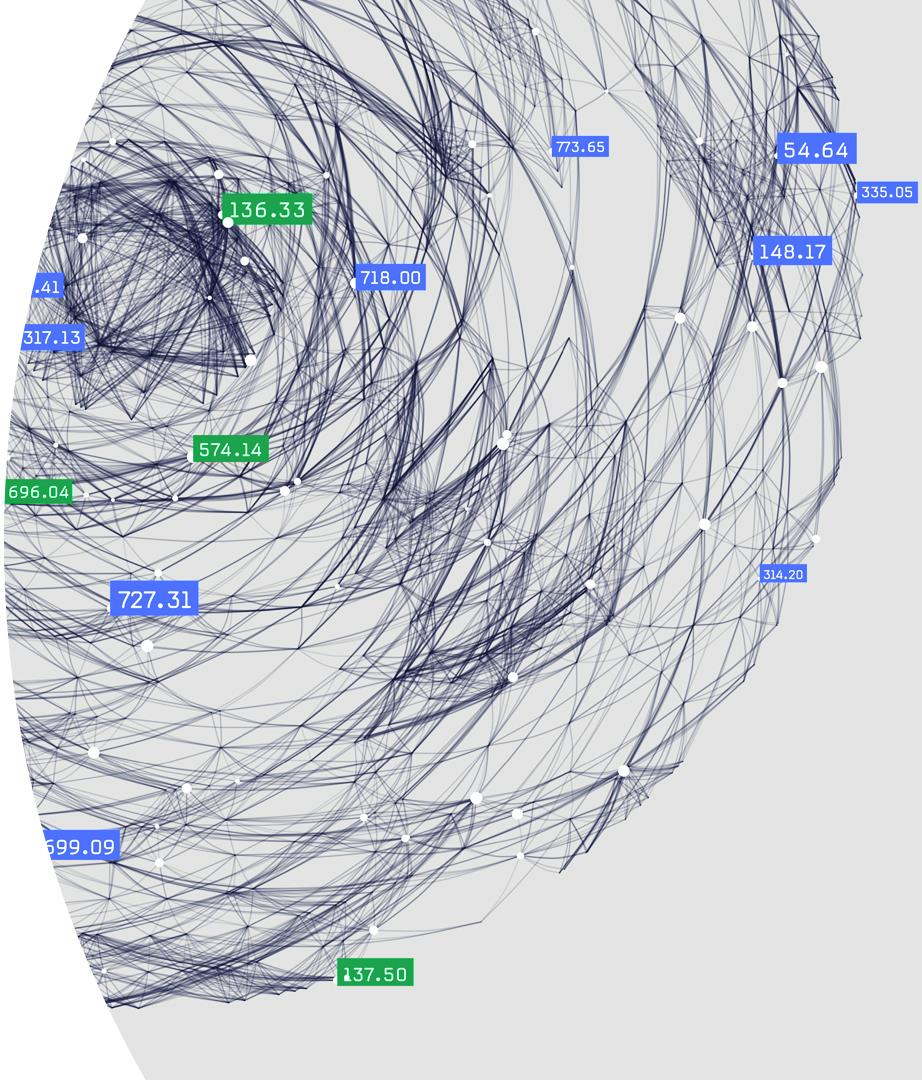
Сотрудники, готовящиеся к увольнению, часто «вытаскивают» корпоративные данные.

Отчёт **показывает информацию о поиске** сотрудником работы.

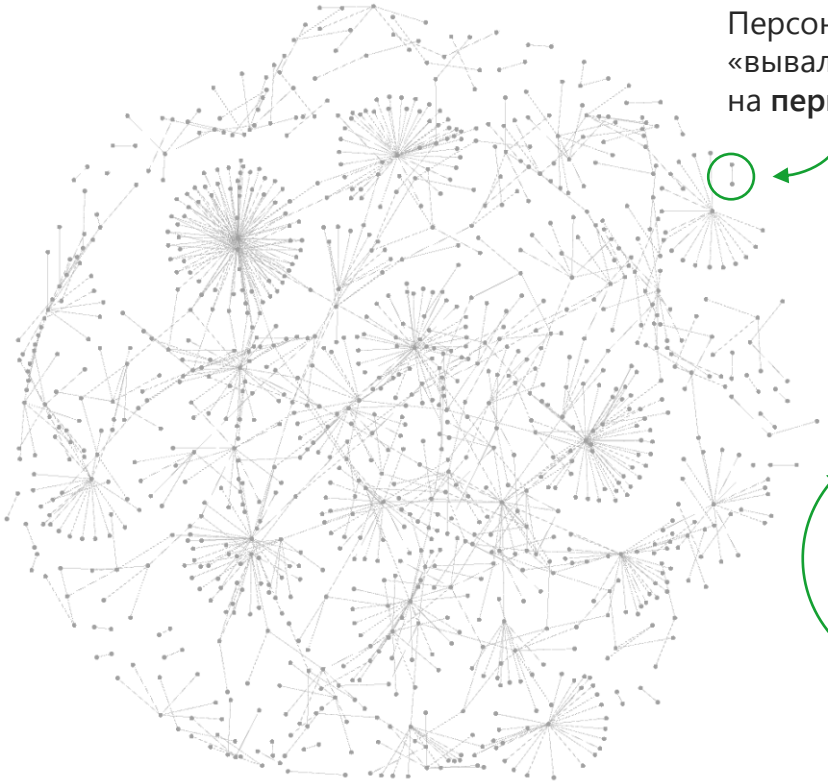
Современные технологии InfoWatch для ИБ

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

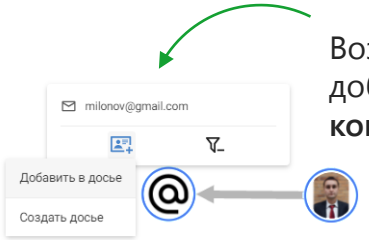
→ **Не только визуальная, но и ПРЕДИКТИВНАЯ аналитика** становятся новой нормой работы служб ИБ



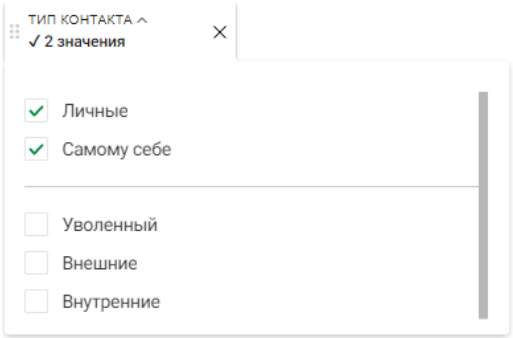
Отслеживание персональных коммуникаций в InfoWatch Vision



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



Возможность добавить **личный контакт** на графе



Фильтр позволяет отобрать все события с личными контактами

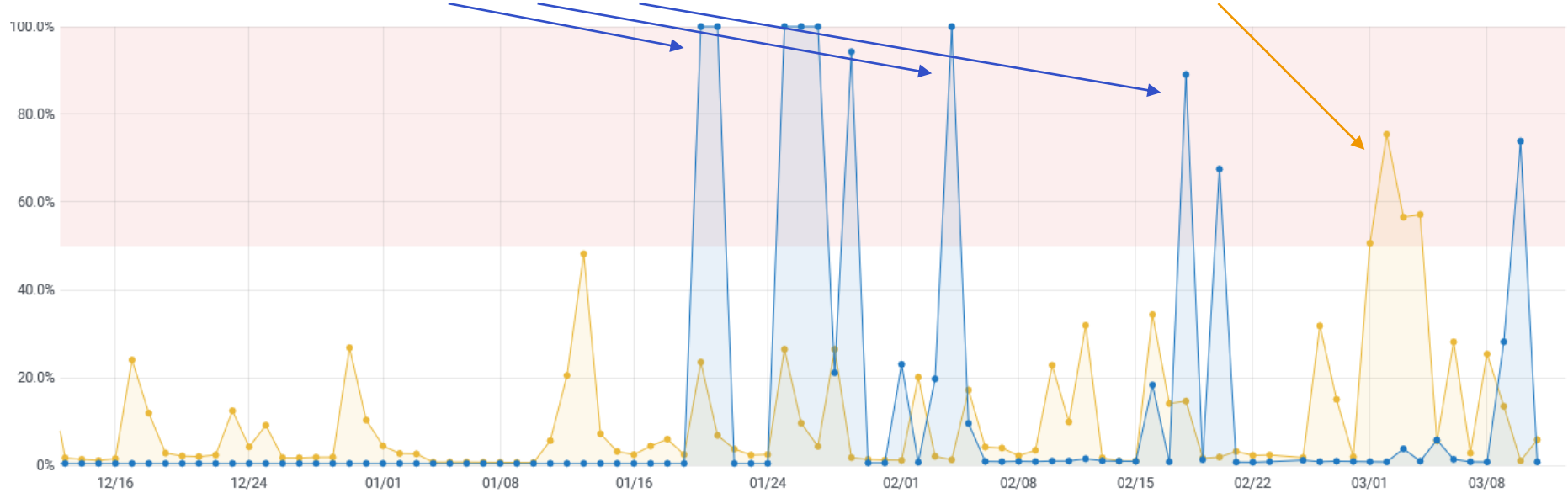
\+ Фильтр **«Уволенные»** позволяет отобразить переписку с бывшими коллегами

Предиктивная аналитика

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

Копирование файлов
на внешние носители

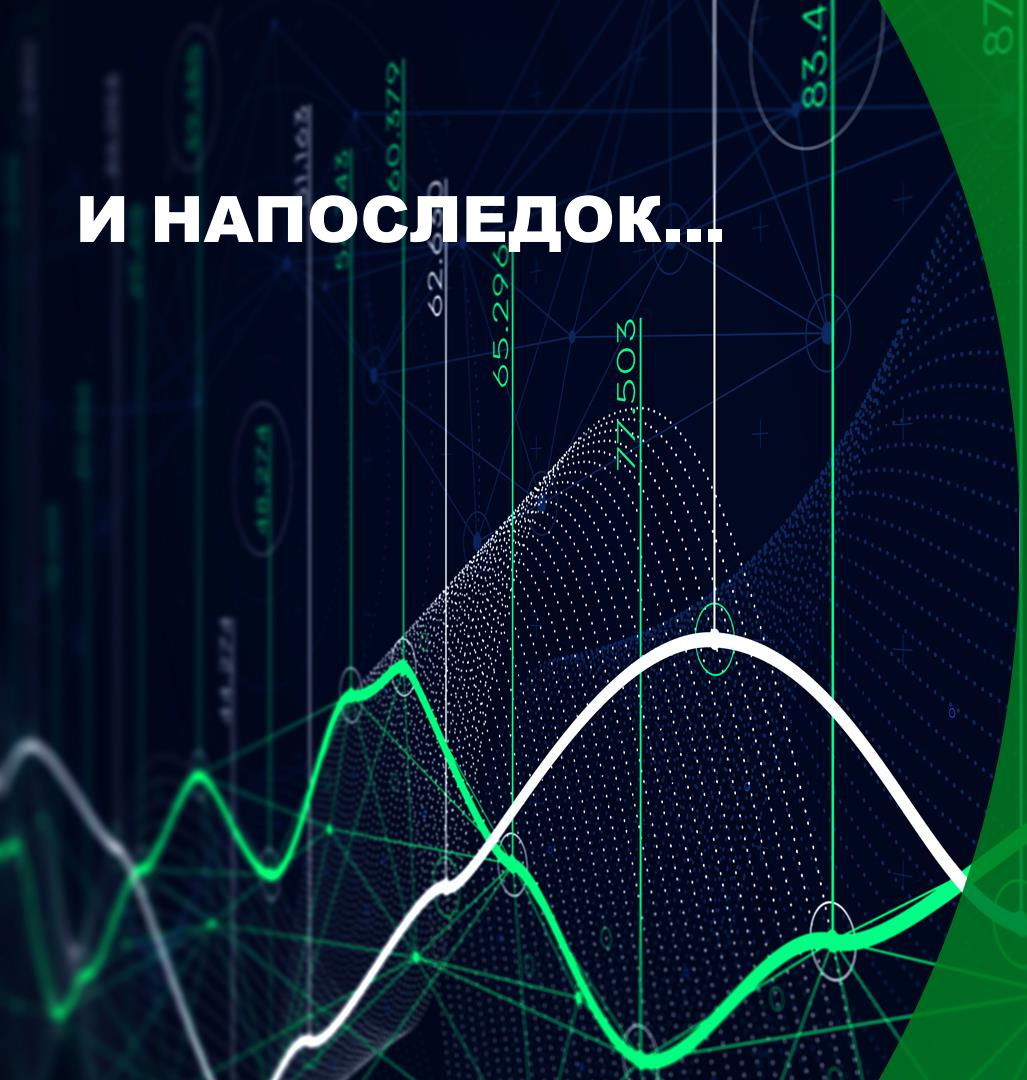
Негативные отзывы
о компании или начальстве



Итог

→ Такие стандартные средства как мониторинг активности и окружения на рабочих местах, мониторинг файловых операций сложно отслеживать вручную на больших объёмах данных

→ **Помочь в этом могут современные средства визуальной и предиктивной аналитики**



И НАПОСЛЕДОК...

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

Первый шаг уже сделан. Дальше? Следите за спойлерами:

/InfoWatchOut /InfoWatch /infowatchnews