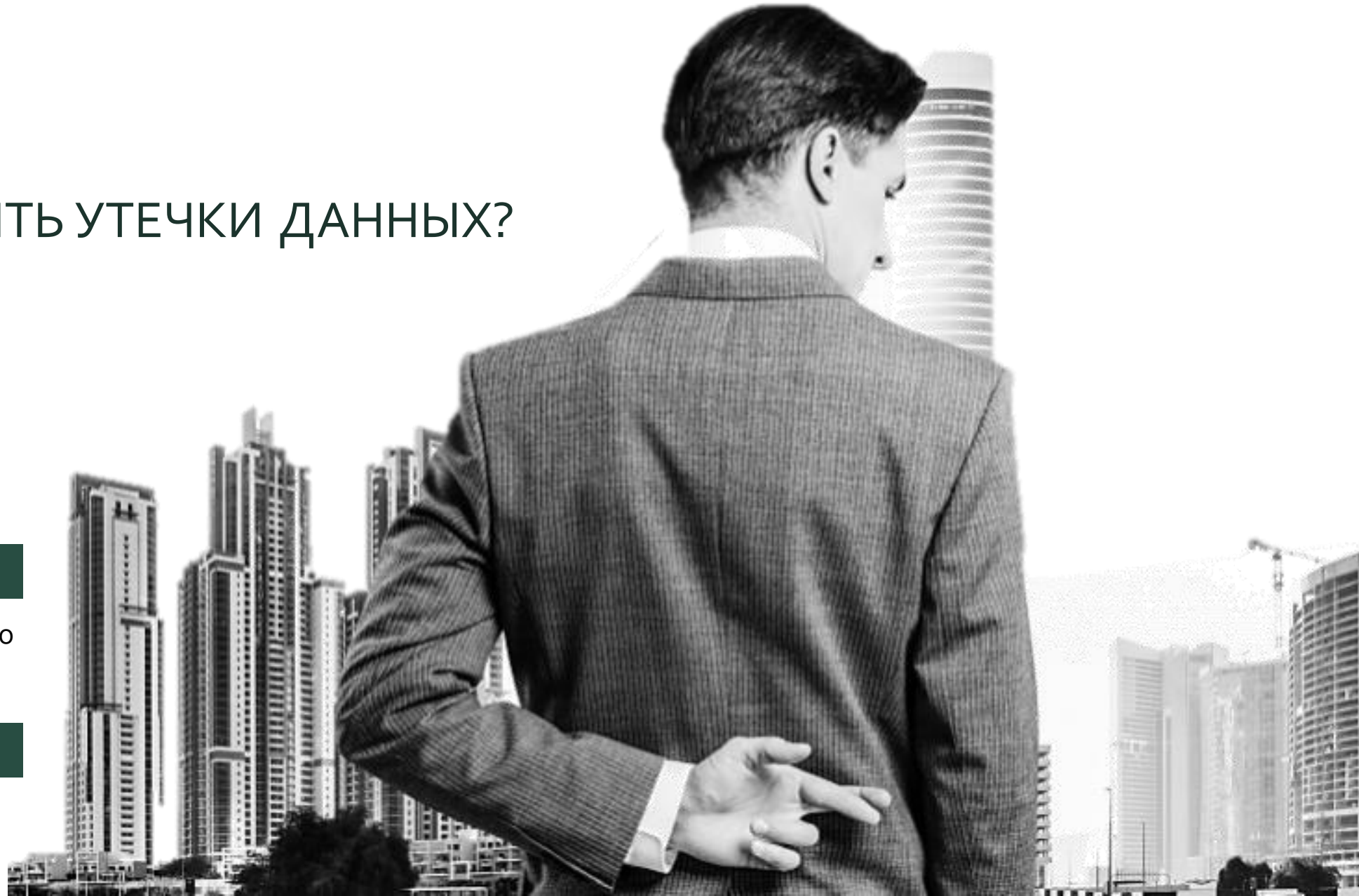
INFOWATCH®

15 ЛЕТ ЗАЩИЩАЕМ ВАШИ ДАННЫЕ

КАК ОСТАНОВИТЬ УТЕЧКИ ДАННЫХ?



Тимур Абдульменов

Руководитель регионального представительства

Мария Чередниченко

Аналитик-эксперт внедрения

ГРУППА КОМПАНИЙ INFOWATCH

ТЕХНОЛОГИЧЕСКИЙ ЛИДЕР

Проверенные решения для защиты данных

15 лет на рынке программных продуктов в сфере информационной безопасности организаций

15 представительств по всему миру: в России и СНГ, на Ближнем Востоке и в Юго-Восточной Азии

500 специалистов и экспертов в области разработки, внедрения и продвижения

ОПЫТ

Свыше 2000 клиентов из 20 отраслей экономики более чем в 20 странах мира

УСЛУГИ

Консалтинг, внедрение, обучение, техническая поддержка

ПАРТНЕРЫ

Партнерская сеть в 20 странах мира

АНАЛИТИЧЕСКИЙ ЦЕНТР

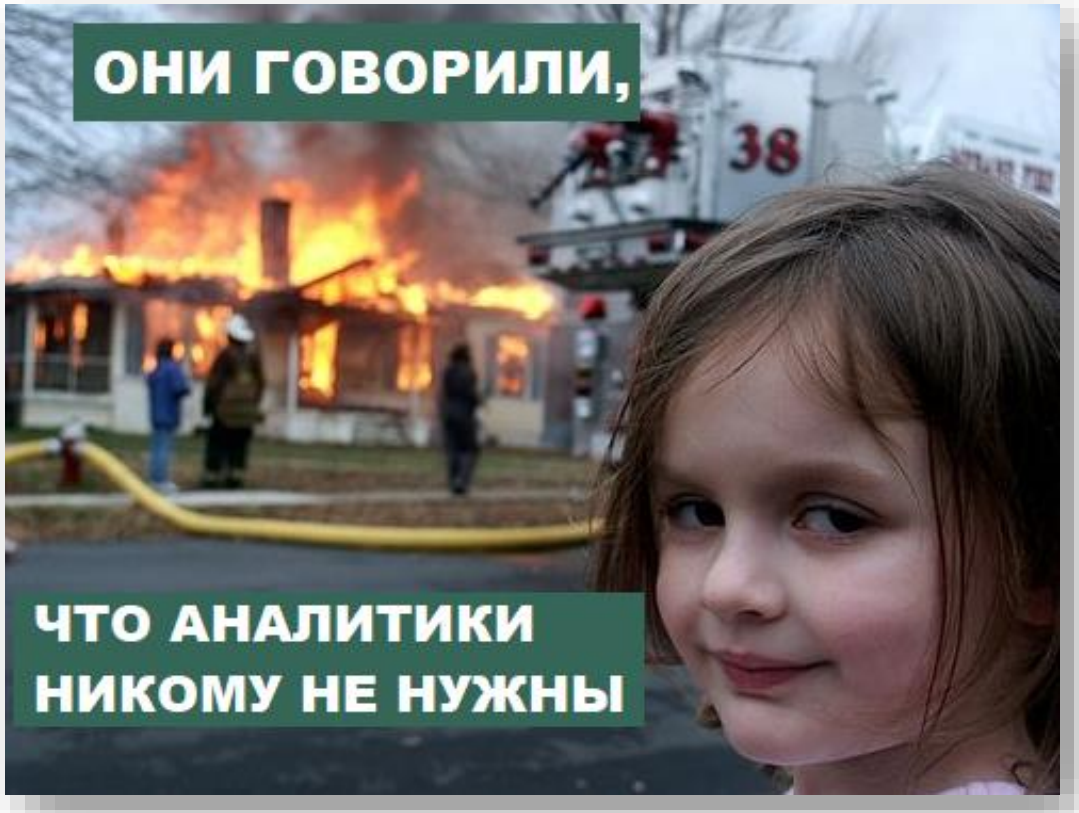
Отчеты о современных угрозах

ЭКСПЕРТИЗА

15 лет практического опыта на рынке информационной безопасности

Мы говорим с Вами на одном языке

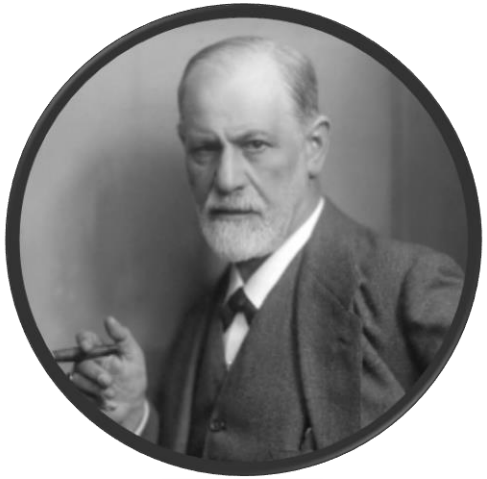
Конечно, сложные аналитические системы мониторинга и защиты информации нужны. Но есть ли у Вас сотрудники, которые будут с ними работать?



ЕЩЕ РАЗ ЛУЧШЕ НАПОМНИТЬ: ПРОЦЕССЫ, ТЕХНОЛОГИИ, КАДРЫ

ПОЧЕМУ РАБОТА АНАЛИТИКА ПРЕВРАЩАЕТСЯ В РАБОТУ ПСИХОЛОГА, ДЕТЕКТИВА И БРОДЯЧЕГО ПРОПОВЕДНИКА

- **Неготовность идеологии** - «казалось бы, зачем спасать людей против их воли?»
- **Неготовность инфраструктуры** - «кстати, о печатных машинках»
- **Неудачный маркетинг** - «могу всё за три копейки»
- **Перфекционизм** - «всё или ничего»



ВНЕДРЕНИЕ DLP

- Инициация
- Предварительное обследование
- Исполнение
- Тестовая эксплуатация
- Завершение

Аналитик понятия не имеет, что происходит

Инженер делает 99% работы

Лингвист обещает помочь, но не помогает

Менеджер по продажам исчезает в самом начале и не появляется до самого конца

УБИРАЕМ ВСЁ И ДОСТАЁМ ДВОЙНЫЕ ЛИСТОЧКИ …
ЭТАП ПРЕДВАРИТЕЛЬНОГО ОБСЛЕДОВАНИЯ

- Кто заинтересован во внедрении **DLP**?
- Какая **КИ** обрабатывается в организации?
- Какая информация «самая ценная», какой её **ЖЦ**?
- Какие особенности корпоративной культуры **ИБ**?

- Какие инциденты уже происходили в организации?
- Какие каналы требуется контролировать?
- Какие меры защиты от внутренних угроз уже реализованы в организации?
- Кому нужен доступ к системе **DLP**?

КОНТРОЛЬ ИНФОРМАЦИОННЫХ ПОТОКОВ - РЕКОМЕНДАЦИИ

П.1

Составьте перечень ИОД

П.2

Составьте правила обработки ИОД

П.3

Уведомьте о мониторинге

П.4

Установите режим защиты ИОД

П.5

Запретите разглашение ИОД (КТ)

П.6

Запретите использование ресурсов в личных целях

П.7

Понимайте, что утечка – не всегда разглашение

П.8

Не используйте сомнительные доказательства

НАБОР ДОКУМЕНТАЦИИ ДЛЯ ОБЕСПЕЧЕНИЯ ЮРИДИЧЕСКОЙ ЗНАЧИМОСТИ

1. «Положение о порядке обращения с информацией ограниченного доступа»
2. «Положение о защите информации ограниченного доступа»
3. «Регламент мониторинга и контроля»
4. «Политика допустимого использования ресурсов»
5. Соглашение о неразглашении информации ограниченного доступа для работников
6. Уведомление/соглашение с работниками на предмет осуществления мониторинга и контроля

Всё сказанное после 5-го бокала – это утечка информации

Ознакомьте сотрудников с документами под роспись!!!

ЧТО ПИСАТЬ В ПОЛИТИКЕ ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ?

Требования по работе со следующими сервисами и средствами обработки и хранения информации:

- Корпоративная электронная почта
- Сеть
- Облачные хранилища
- Персональная электронная почта
- Внешние носители
- Корпоративные рабочие станции

«Я дома хочу поработать»

«Я к этой программе привык, много лет её использую»

«Через рабочую почту не могу отправить файлы большого размера»

- Корпоративные мобильные устройства
- Персональные мобильные устройства
- Сервисы мгновенных сообщений
- Удаленный доступ
- Многофункциональные устройства
- Файловые хранилища

АНАЛИТИЧЕСКИЕ РАБОТЫ – КОНЦЕПЦИЯ НАСТРОЙКИ СИСТЕМЫ

Определить цели Заказчика

Выявить сотрудников, входящих в группу риска

Определить перечень, формат и маршруты передачи важной информации

Определить политики безопасности, действующие в компании

Определить настройки системы - Концепция

ЛОГИКА РАБОТЫ INFOWATCH TRAFFIC MONITOR

① Сбор и перехват

Система собирает и перехватывает любые события, генерируемые сотрудниками компании

② Анализ

Система использует инструменты анализа для детектирования конфиденциальных данных в потоке событий (автоматически определяется категория и тематика)

③ Принятие решений

Реакция на событие (блокировка, уведомление) и определение уровня угрозы

④ Сохранение в базу

Все события хранятся в одном архиве как доказательная база для расследования инцидентов

② Анализ

Лингвистический анализ

Детектор текстовых объектов

Детектор эталонных документов

Детектор графических объектов

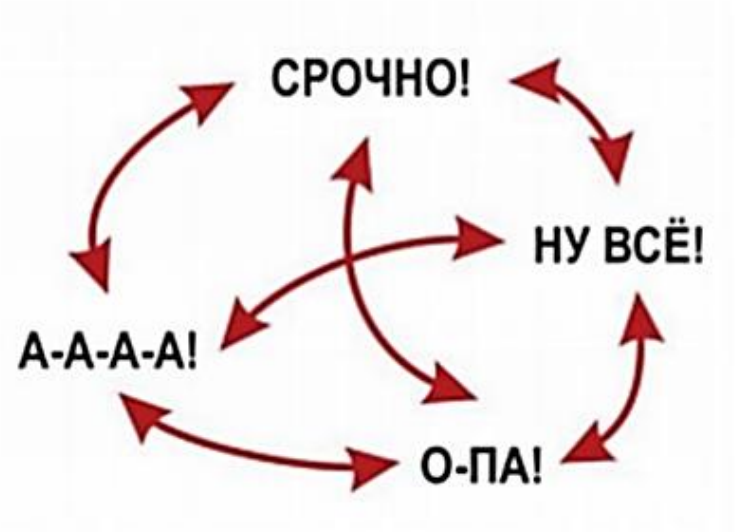
Детектор выгрузок из баз данных

Детектор заполненных бланков

③ Принятие решений

- Направление маршрута
- Тип события
- Компьютеры
- Отправители/ Получатели

Когда случается инцидент ИБ...



- Отправка почтовых уведомлений
- Назначение вердикта
- Назначения уровня нарушения
- Назначения статуса/тега

→ **Отчетность**

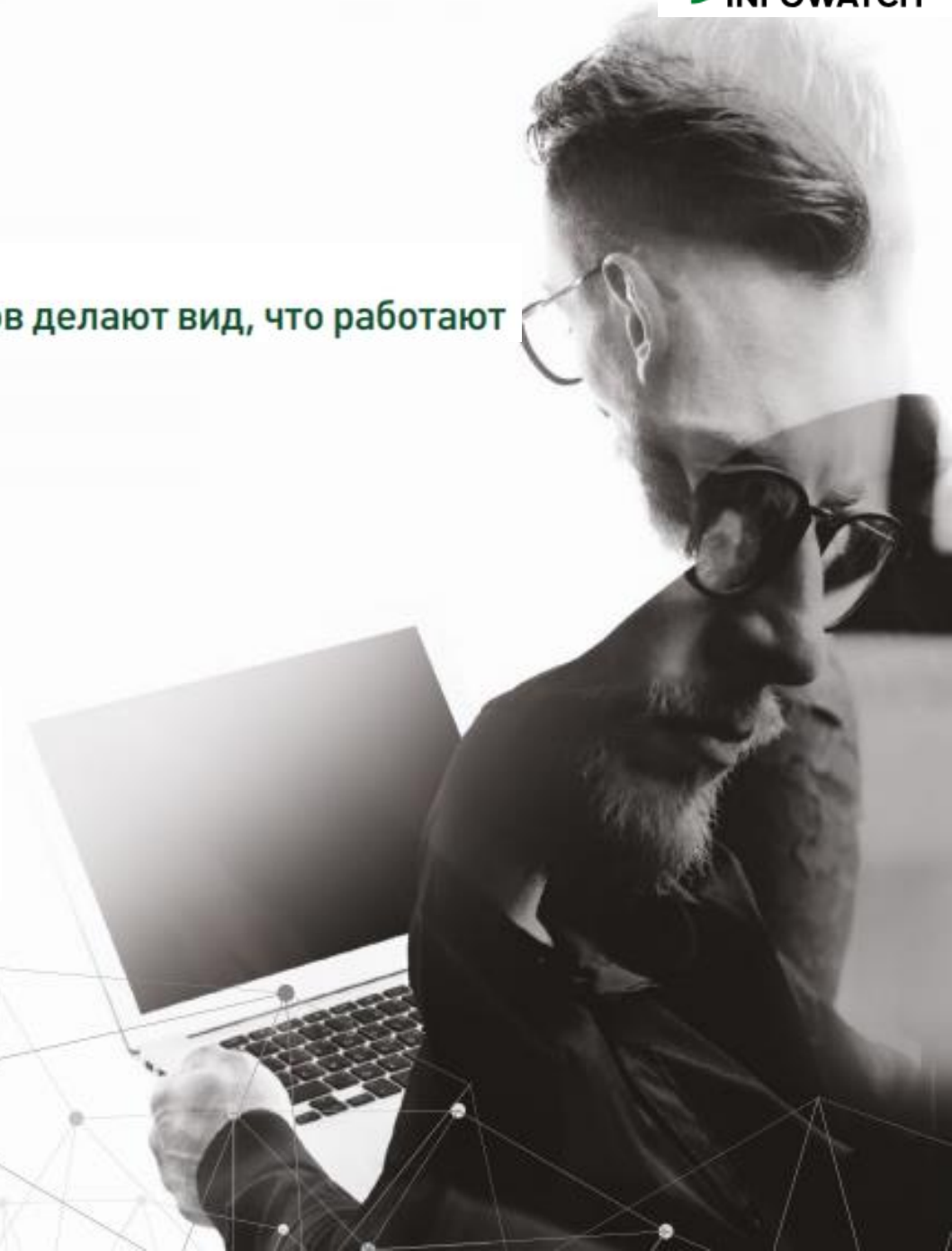
INFOWATCH
PERSON MONITOR

INFOWATCH

КАК МОЖНО СНИЗИТЬ РИСКИ С ПОМОЩЬЮ МОНИТОРИНГА ПЕРСОНАЛА

61% утечек — результат действий инсайдеров

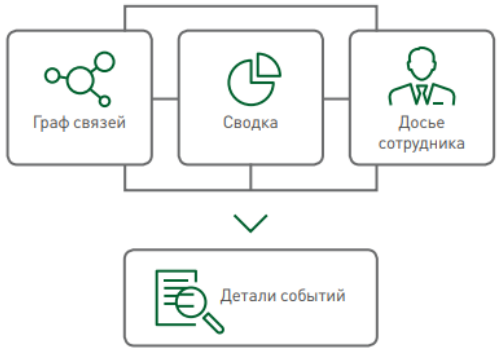
почти **85%** сотрудников делают вид, что работают

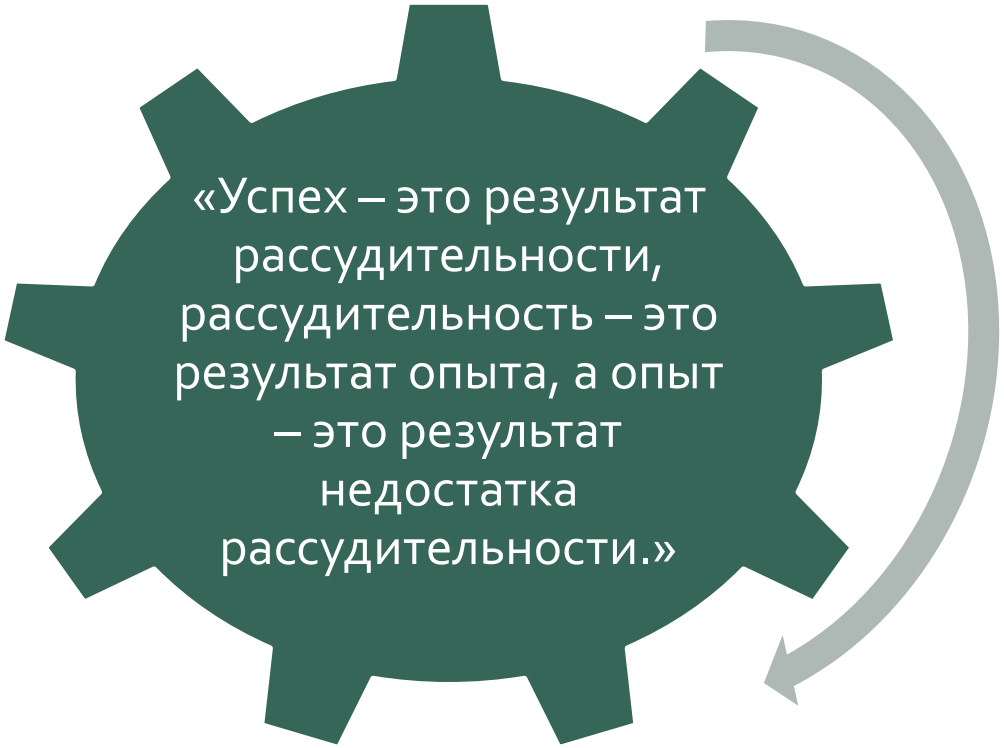


- Отслеживайте взаимодействие сотрудников с ИТ-ресурсами
- Ведите мониторинг рабочей активности, подозрительных и опасных действий
- Выявляйте неэффективных сотрудников и факты нерационального использования рабочего времени

РАБОТА С КОНТЕНТОМ

1. **Не игнорируйте** заблокированные инциденты
2. **Не игнорируйте** повторяемые инциденты
3. **Определитесь** с форматом уведомлений
4. **Обращайте внимание** на контекст
5. **Анализируйте** релевантность индикаторов
6. **Проводите** ретроспективный поиск
7. Критичное **блокируйте** превентивно
8. **Проверяйте** на себе и своем контенте





О ЧЕМ ГОВОРИЛИ? ВСПОМНИТЬ ВСЕ:

Настройки и правила DLP нужно «заточить» под свои задачи

Необходимо вовлечение сотрудников в работу с DLP

Следует определить и проработать варианты «управленческого решения» еще до инцидента

Документировать вопросы ИБ, связанные с DLP не так сложно

Полезные материалы можно получить у **InfoWatch**

INFOWATCH®

15 ЛЕТ ЗАЩИЩАЕМ
ВАШИ ДАННЫЕ

СПАСИБО ЗА ВНИМАНИЕ!