



# INFOWATCH PERSON MONITOR

Мониторинг  
действий сотрудников  
для проведения  
внутреннего  
расследования

## 51%

Основная причина  
утечек — результат  
умышленные действия  
внутренних нарушителей \*

Статистика утечек  
данных в мире в 1/2 2022

Экспертно-аналитический центр  
InfoWatch, 2023



**Сотрудники становятся нарушителями по разным причинам: от шпионажа в пользу конкурентов и жадности наживы до извечного любопытства, по элементарному незнанию, из-за глупой ошибки или небрежности.**

Независимо от мотива, удар, который наносит доверенный инсайдер, имеющий доступ к конфиденциальной информации, оказывается наиболее болезненным, а последствия — разрушительными.

## Как установить нарушителя и собрать необходимые доказательства?

**InfoWatch Person Monitor** — система мониторинга персонала, которая собирает данные о действиях сотрудника на рабочем месте и предоставляет аналитические отчёты для службы информационной или кадровой безопасности.

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

Восстановить полную картину событий в ходе инцидента

Доказать вину попавшего под подозрение или убедиться в его непричастности

Проконтролировать действия привилегированных пользователей

## Собрать максимум информации о действиях пользователя

- Входящие и исходящие сообщения электронной почты, вложенные файлы
- Мониторинг коммуникаций в мессенджерах Lync, Skype, Viber, Telegram, WhatsApp, Bitrix24, Slack, Myteam (mail.ru), Cisco Webex Teams, Telegram Desktop 2.4 + и т. д.\*
- Посещаемые сайты и интернет-запросы, передача файлов через файлообменники, веб-почту и чаты
- Запись скриншотов и видео с экрана, изображения с веб-камеры, звука с микрофона и динамиков
- Детектирование фактов съёмки экрана мобильным устройством
- Распознавание лиц с веб-камер для контроля присутствия и идентификации сотрудников
- Статистика использования приложений и мониторинг вводимого текста
- Операции с документами: удаление, печать, копирование на внешние носители и в облако
- Расширение возможностей мониторинга на ПК под управлением MacOS и Astra Linux
- Факт присутствия на рабочем месте и в офисе, время, проведенное за компьютером
- Геолокация мобильных устройств и ноутбуков на платформах Android, Windows 10

\*Список поддерживаемых мессенджеров постоянно расширяется, обязательно запросите актуальный вариант у специалиста InfoWatch

# Проанализировать данные и вынести обоснованное решение

Простые и интуитивные графические отчёты визуализируют собранную информацию и позволяют получить ясную картину: восстановить последовательность действий сотрудника и выявить характер его активности.

IW\Ivanov (Иванов Иван Иванович) | Суммарное время активной работы ~87% (7ч21м)

#	Заголовок окна приложения	Активное время	Общее время
	ТУ_новый-проект_правки_ИИ.doc «Microsoft Word»   %ProgramFiles%\Microsoft Office\Office14\WINWORD.EXE   2019-05-31, 15:56:52 <a href="#">Показать/скрыть вводимый текст</a>	12% (1ч00м)	12% (1ч01м)
	PersonMonitor_with_TechSupport.xlsx «Microsoft Excel»   %ProgramFiles%\Microsoft Office\Office14\EXCEL.EXE   2019-05-31, 09:40:21 <a href="#">Показать/скрыть вводимый текст</a>	11% (0ч55м)	11% (0ч56м)
	Входящие — Ivan.Ivanov@company.com «Microsoft Outlook»   %SystemDrive%\PROGRAM*1\MICROS*1\Office14\OUTLOOK.EXE   2019-05-31, 09:36:08 <a href="#">Показать/скрыть вводимый текст</a>	10% (0ч50м)	10% (0ч51м)
	Презентация.pptx «Microsoft PowerPoint»   %ProgramFiles%\Microsoft Office\Office14\POWERPOINT.EXE   2019-05-31, 17:34:44 <a href="#">Показать/скрыть вводимый текст</a>	10% (0ч48м)	10% (0ч48м)

## Предъявить законно собранные доказательства и не оставить злоумышленника безнаказанным

При использовании системы мониторинга персонала эксперты **InfoWatch** рекомендуют придерживаться основных правил:

**Задокументируйте правила работы** с информацией и бизнес-приложениями в организации

**Уведомите сотрудников** о возможности ведения мониторинга

**Определите аргументированную цель** применения средств мониторинга к конкретному работнику в процессе служебного расследования. Необоснованное применение, неадекватно выбранная глубина и способ мониторинга могут нарушить права работников

### Важно помнить!

Письменное согласие работника на мониторинг его действий не имеет силы перед статьей 17, ч. 2 Конституции РФ. Мы рекомендуем разрабатывать методологию применения системы мониторинга исключительно в привязке к корпоративным ресурсам. Сотрудники должны быть оповещены обо всех ограничениях. Консультанты и юристы **InfoWatch** сопровождают проекты по внедрению продуктов компании и помогут грамотно выстроить процессы и разработать политики безопасности в организации, обеспечить легитимную работу средств защиты информации и мониторинга сотрудников.

## DLP и система мониторинга персонала: не замена, а дополнение

Система защиты от утечек Data Loss Prevention (DLP) может предотвратить утечку конфиденциальных данных из организации и просигнализировать об инциденте. **InfoWatch Person Monitor** дополняет картину исчерпывающей информацией о действиях конкретных сотрудников, раскрывает контекст и предоставляет доказательства вины. Только совместное использование двух систем создаст полноценную защиту интересов организации.

DLP-система	Система мониторинга персонала
Контроль информационных потоков	Контроль действий сотрудников
Выявление инцидентов информационной безопасности, связанных с передачей данных	Выявление инцидентов информационной безопасности на основе анализа действий сотрудников
Блокировка утечек конфиденциальных данных	Сбор доказательной базы при расследованиях

# Какая картина откроется вам?

По статистике InfoWatch, в 87% случаев в ходе пилотного проекта организации обнаруживают нарушения, которые требуют принятия немедленных мер.

Свяжитесь с экспертами InfoWatch для запуска пилотного проекта в вашей организации:

[sales@infowatch.ru](mailto:sales@infowatch.ru)

[pm.infowatch.ru](http://pm.infowatch.ru)

+7 495 22 900 22



InfoWatch — ведущий российский разработчик решений для обеспечения информационной безопасности организаций. Мощная академическая база, лучшие инженеры, математики и лингвисты с 2003 года обеспечивают технологическое преимущество InfoWatch в области защиты предприятий от современных киберугроз, информационных и инсайдерских атак.

Признанный эксперт и лидер рынка России и СНГ в области защиты корпоративных данных InfoWatch успешно выполнил более 3000 проектов для коммерческих и государственных организаций в 20-ти странах мира.

Две трети из 50-ти крупнейших компаний России (в соответствии с рейтингом «Эксперта») доверили InfoWatch выполнение масштабных и, зачастую, нестандартных проектов, связанных с информационной безопасностью. Причина такого доверия — не только высокое качество и уникальность технологий, но и чувство уверенности, которое возникает от сотрудничества с InfoWatch благодаря сопровождению клиентов на всех этапах проектных работ.

 /InfoWatchOut

 /InfoWatch



Министерство  
обороны Российской  
Федерации



Федеральная  
таможенная  
служба



Фонд  
социального  
страхования



Федеральная  
налоговая  
служба



Полное или частичное копирование материалов возможно только при указании ссылки на источник, сайт [infowatch.ru](http://infowatch.ru), или на страницу с исходной информацией.