Опыт и технологии ГК InfoWatch по защите данных

Высоцкий Павел
Менеджер по развитию бизнеса в ЦФО

Москва, 2019

О ГК ИнфоВотч

InfoWatch
более 15 лет
на рынке

Один из крупнейших
ИБ-производителей
России

Лучшее российское
решение по версии
Gartner

Собственные
запатентованные
технологии

В реестре
отечественного
ПО

2000 клиентов
2/3 топ-50 рейтинга
«Эксперт-400»

Некоторые клиенты

INFOWATCH®

НЕФТЕГАЗОВЫЙ СЕКТОР

- Газпром ВНИИГАЗ
- СлавНефть
- Транснефть
- ОАО «ВНИПИгаздобыча»

ЭНЕРГЕТИКА

- e·on
- Интер РАО Каширская ГРЭС
- ТВЭЛ
- ОДК

ПРОМЫШЛЕННОСТЬ

- Московский вертолетный завод им. М.Л. Миля
- ОСК
- Tira
- Оборонпром

ТЕЛЕКОММУНИКАЦИИ

- МТС
- МегаФон Таджикистан

БАНКИ

- Сбербанк
- Райффайзен Банк
- Банк Форштадт
- Банк Кольцо Урала
- Связь Банк
- Home Credit Bank

СТРАХОВЫЕ КОМПАНИИ

- СОГАЗ страховая группа
- ВСК страховой дом

ГОСУДАРСТВЕННЫЙ СЕКТОР

- Федеральная налоговая служба
- Федеральная таможенная служба
- Министерство обороны Российской Федерации
- Фонд социального страхования

ТРАНСПОРТ И ЛОГИСТИКА

- Росжелдорпроект
- Газпром Авиа
- SPSR express

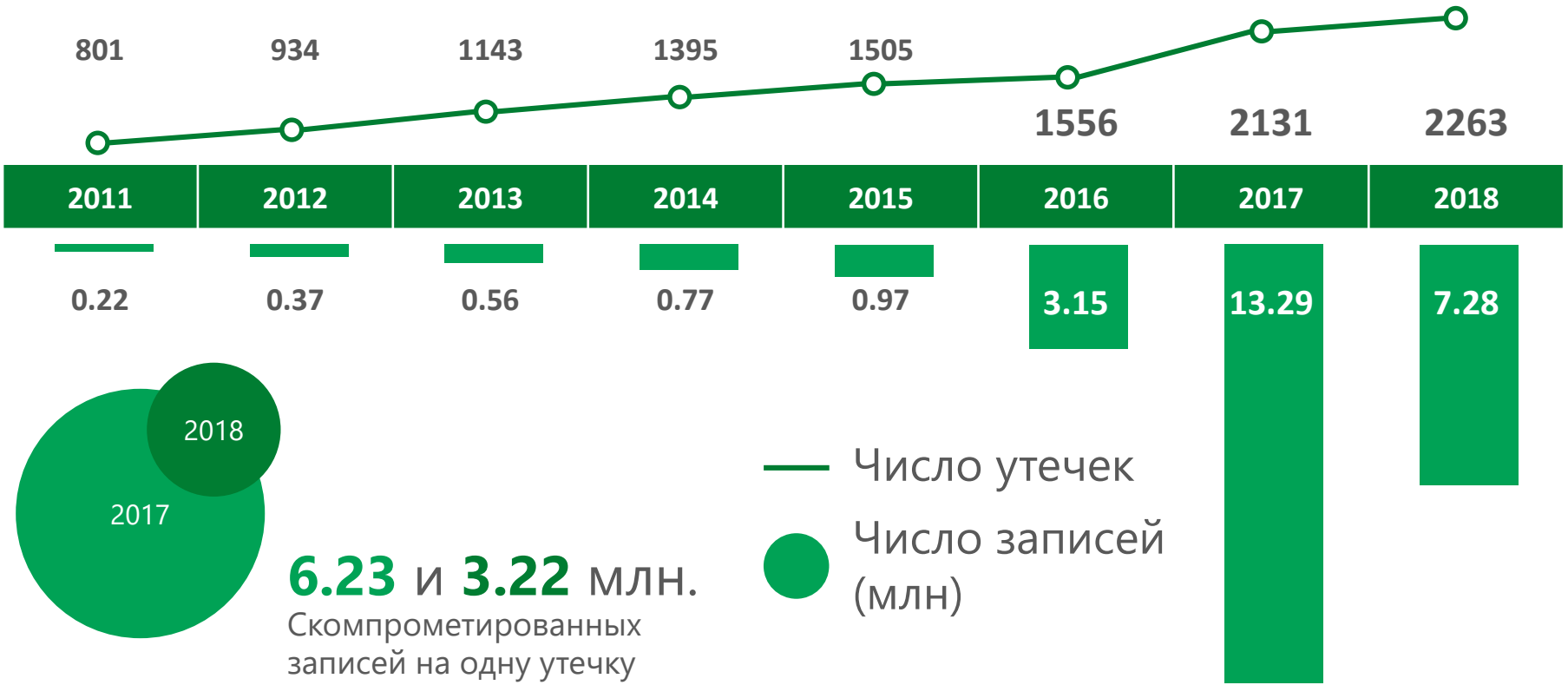
МЕДИЦИНА И ФАРМАЦЕВТИКА

- STADA
- Ниармедик

ТОРГОВЛЯ

- Fix price
- Магнит
- О'кей
- KUPIVIP.RU

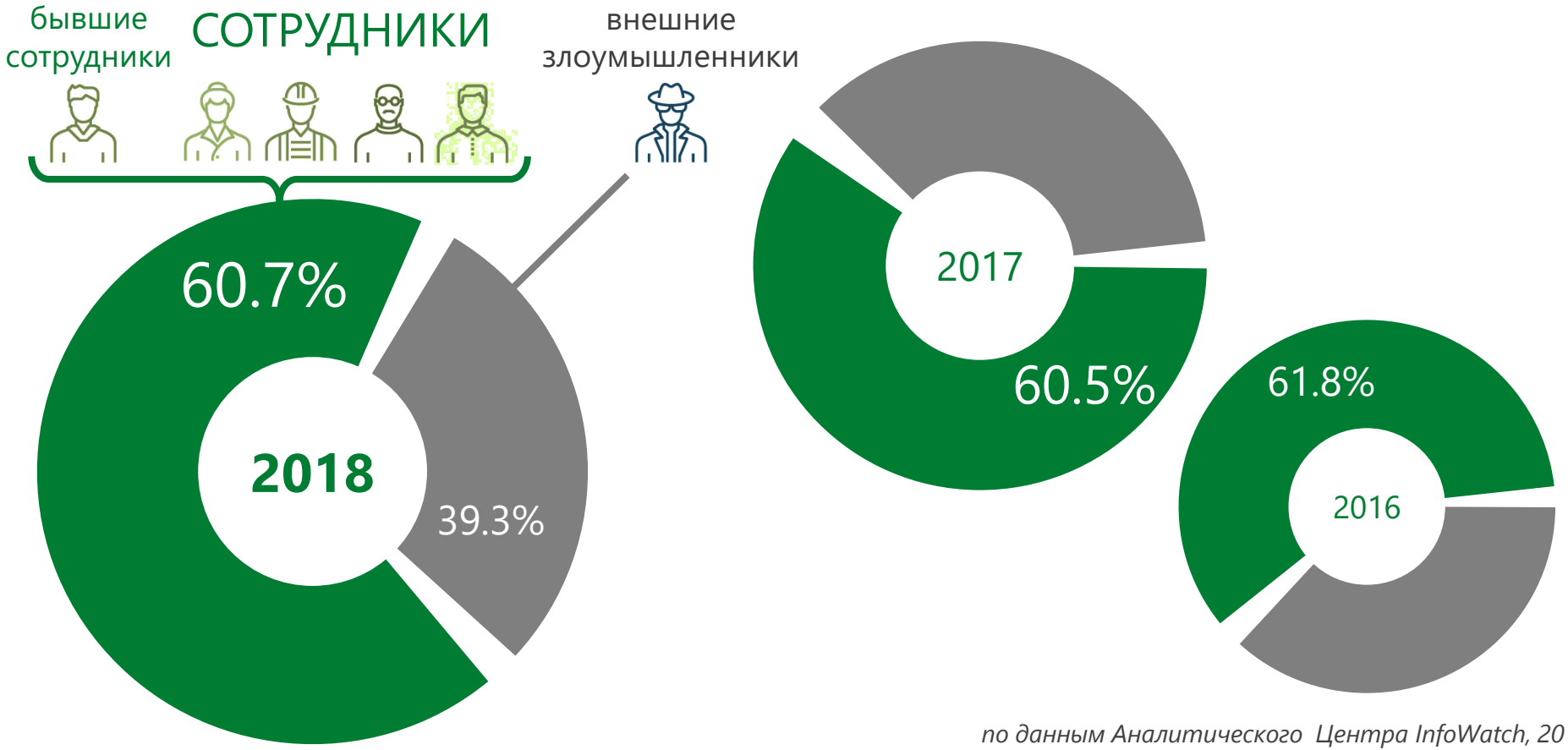
Утечки набирают скорость



6.23 и **3.22** млн.
Скомпрометированных записей на одну утечку

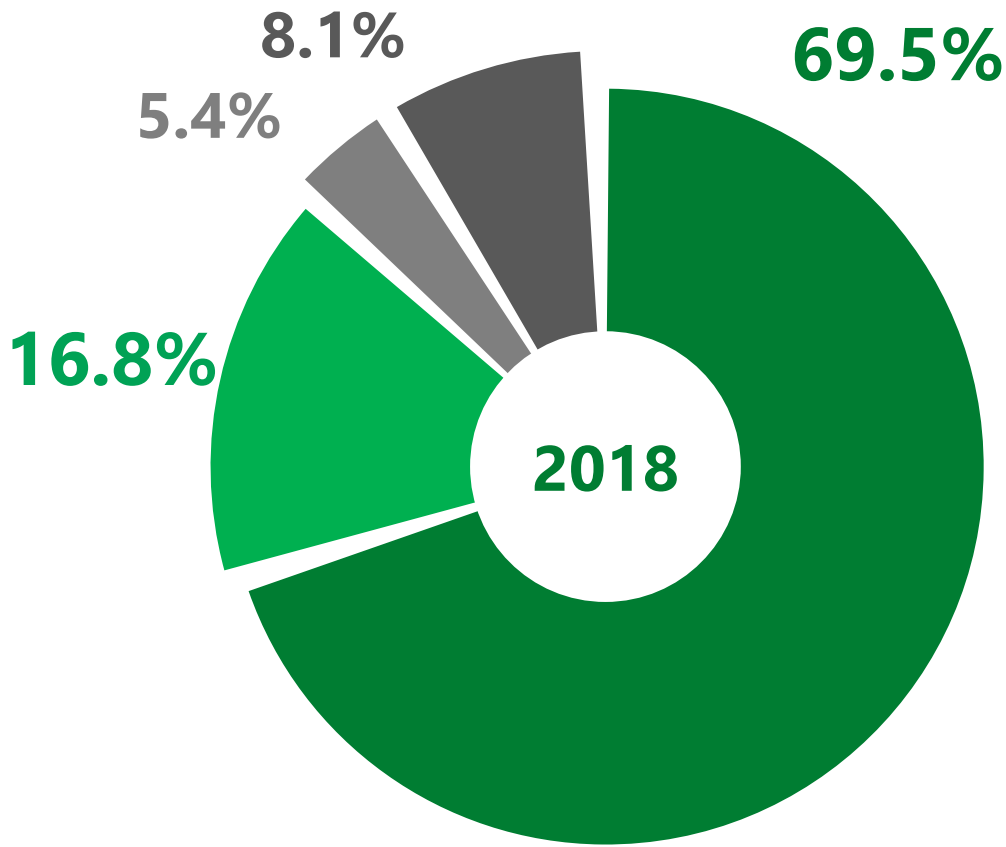
по данным Аналитического Центра InfoWatch, 2019

Источники утечек



по данным Аналитического Центра InfoWatch, 2019

Случайные и организованные утечки



- Персональные данные
- Платежная информация
- Государственная тайна
- Коммерческая тайна

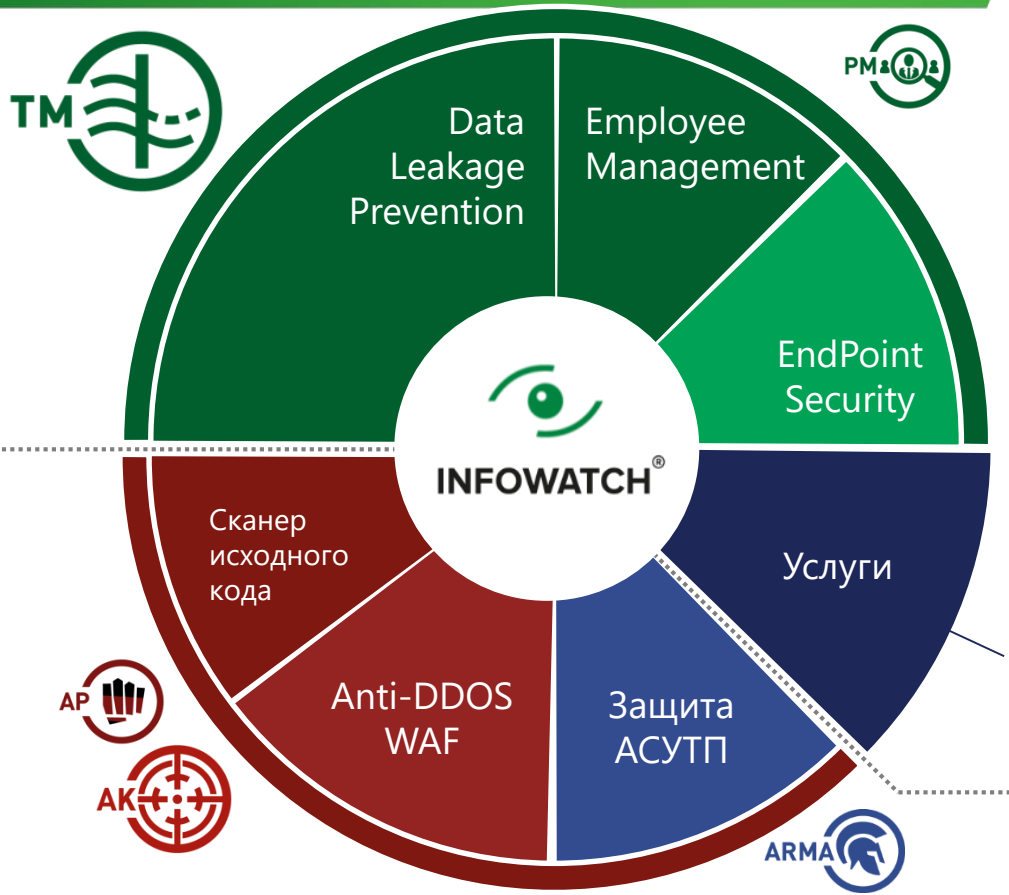
по данным Аналитического Центра InfoWatch, 2019

Продукты ГК InfoWatch

INFOWATCH®

от внутренних угроз

от внешних угроз



консалтинг
обучение
техподдержка

INFOWATCH®

TRAFFIC MONITOR

Защита от утечек информации

Определяет содержимое файлов

Использует комбинации технологий

Выявляет сговоры и мошеннические схемы

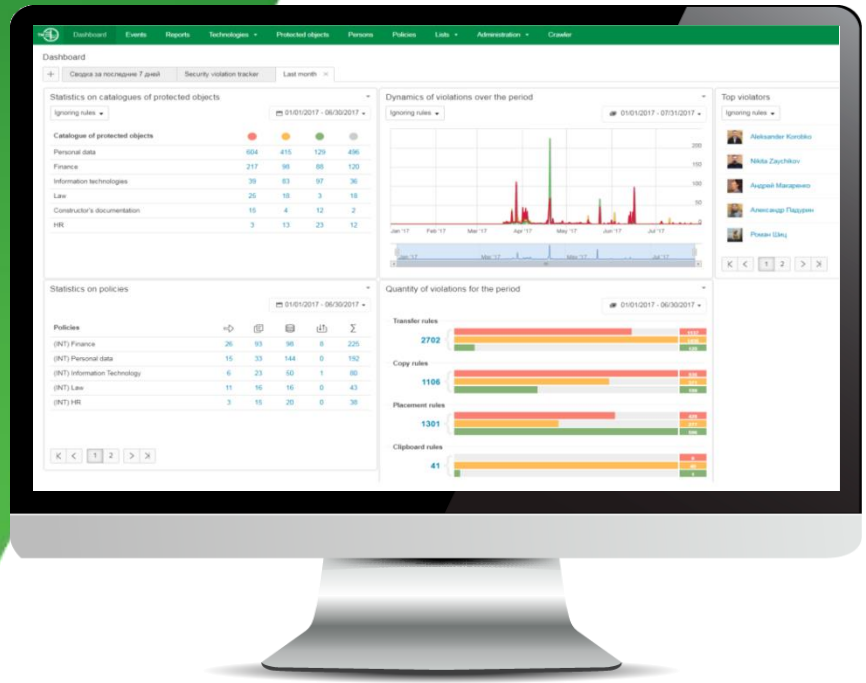


Схема работы

INFOWATCH®

Перехват

Анализ

Решение

Хранение

ПРАВОВЫЕ требования и задачи

INFOWATCH

Коммерческая тайна ← 98-ФЗ

Информация в АСУ ТП ← Приказ ФСТЭК России № 31 ← 187-ФЗ

Персональные данные ← ПП 1119 ← Приказ ФСТЭК России № 21 ← 152-ФЗ

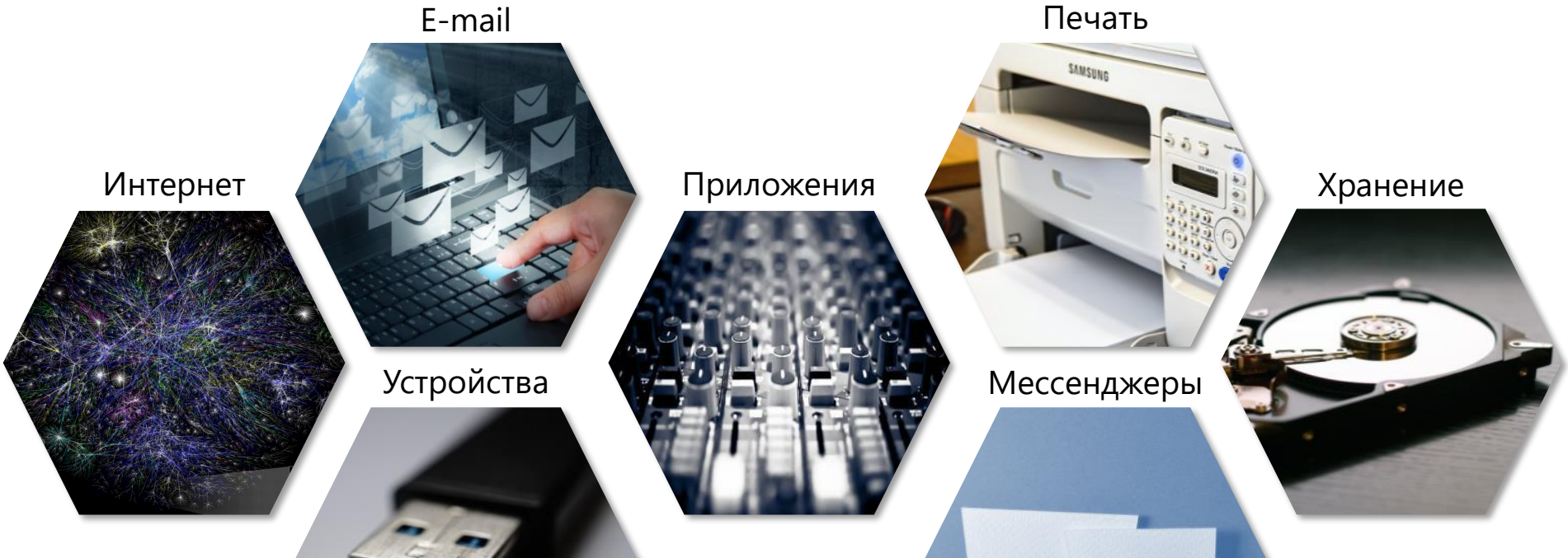
Государственные информационные системы ← ПП 211 ← Приказ ФСТЭК России № 17 ← 149-ФЗ

Методические рекомендации ФСТЭК России

Инвентаризация и **категоризация** информационных активов	**Мониторинг** и **контроль** передаваемой информации	Контроль **подключения** к сетям **общего пользования**
Контроль использования **съемных носителей**	**Выявление** и контроль **мест хранения** информации	Анализ **событий** и управление **инцидентами**

ШАГ 1: Перехват

Помимо возможности использовать сторонние решения для перехвата данных разработаны **собственные средства контроля**:



Перехват

Почта:
SMTP(S), MAPI, IMAP4(S), POP3(S), NRPC (Lotus)

Интернет:
HTTP(S), веб-почта, форумы, облачные хранилища и др

Мессенджеры:
Telegram, чат VK и FB, Jabber и др. XMPP-мессенджеры

Съемные носители и внешние устройства:
USB, HDD, FireWire, Wi-Fi, Bluetooth, Мобильные устройства (MTP) и др.

Печать:
Локальные и сетевые принтеры, печать в терминальных сессиях

Приложения:
Запуск, копирование в буфер обмена, снимки экрана, печать

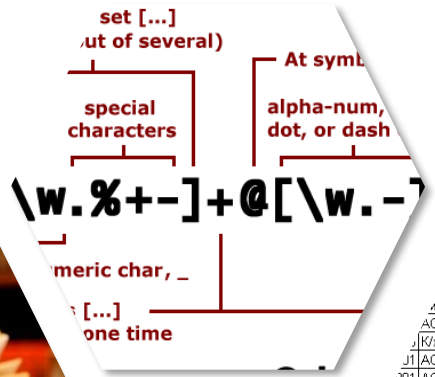
Подключения к внешним сетям

Копирование файлов на сетевые ресурсы FTP и SMB

ШАГ 2: Анализ

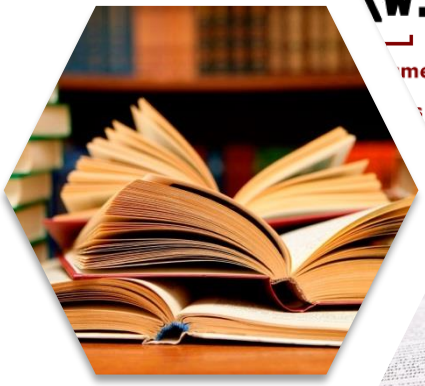
Используются **комбинации** технологий для анализа **текста**, **изображений**, **выгрузок БД** и файлов любых форматов:

Шаблоны



Бланки и анкеты

Лингвистика



Таблицы

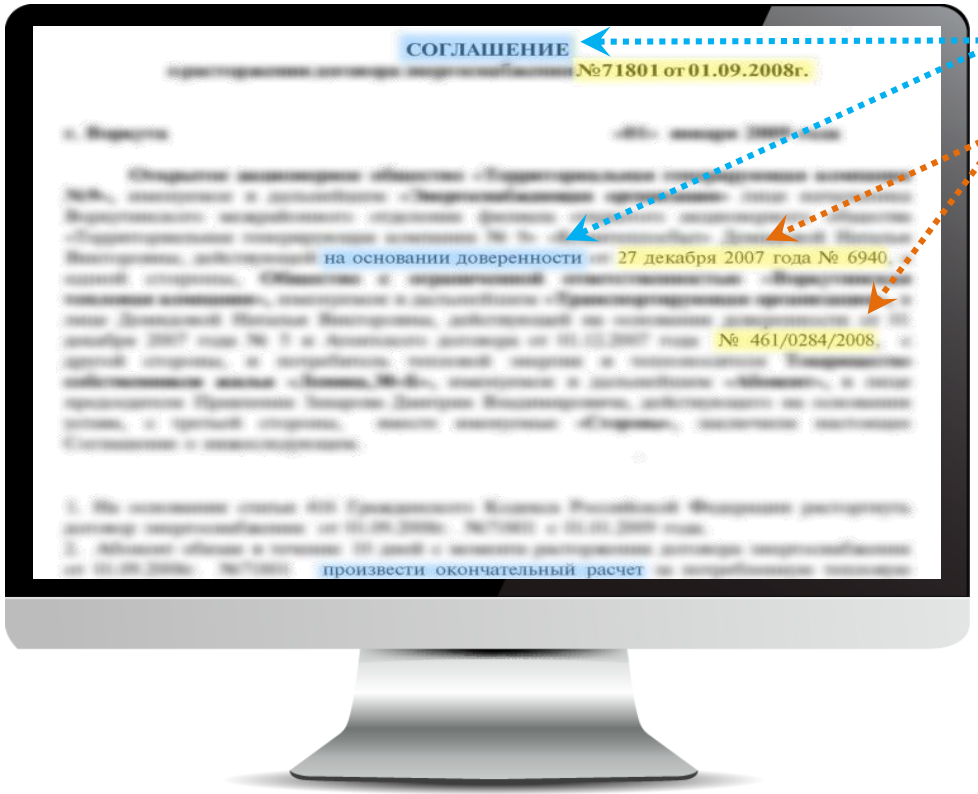
	B	C	D	E
	анизация	Дата	Товар	Ед.изм.
	ЛЬЯНС"	1.Янв	соль	кг
	"Белокуриха"	1.Янв	сахар	кг
	ЗТ "Белокуриха"	3.Янв	хлеб	бул.
	йск.маслосырзавод	3.Июн	сода	пач.
	АОЗТ "Белокуриха"	4.Янв	сок	бан.
	К/х "ЗАРЯ"	4.Янв	пиломат.	метр
	АО "АЛЬЯНС"	13.Янв	лимоны	кг
001	АО "АЛЬЯНС"	3.Фев	компьютер	шт.
002	АОЗТ "Белокуриха"	12.Фев	Хлеб	бул.
003	Бийск.маслосырзавод	12.Фев	бензин	л
	АОЗТ "Белокуриха"	2.Мар	сода	пач.
	К/х "ВОСТОК"	2.Мар	апельсины	кг
	"ЗАРЯ"	5.Мар	апельсины	кг
	"ЛУЧ"	4.Апр	апельсины	кг
	ЗАРЯ"	6.Апр	мука	кг
	ОСТОК"	6.Май	сахар	кг
	СТОК"	13.Июн	лимоны	кг
	ТОК"	13.Июн	хлеб	бул

Детекторы

Изображения

Обучаемость

Анализ



термины и фразы

текстовые объекты

ABBYY OCR

Более 40 языков

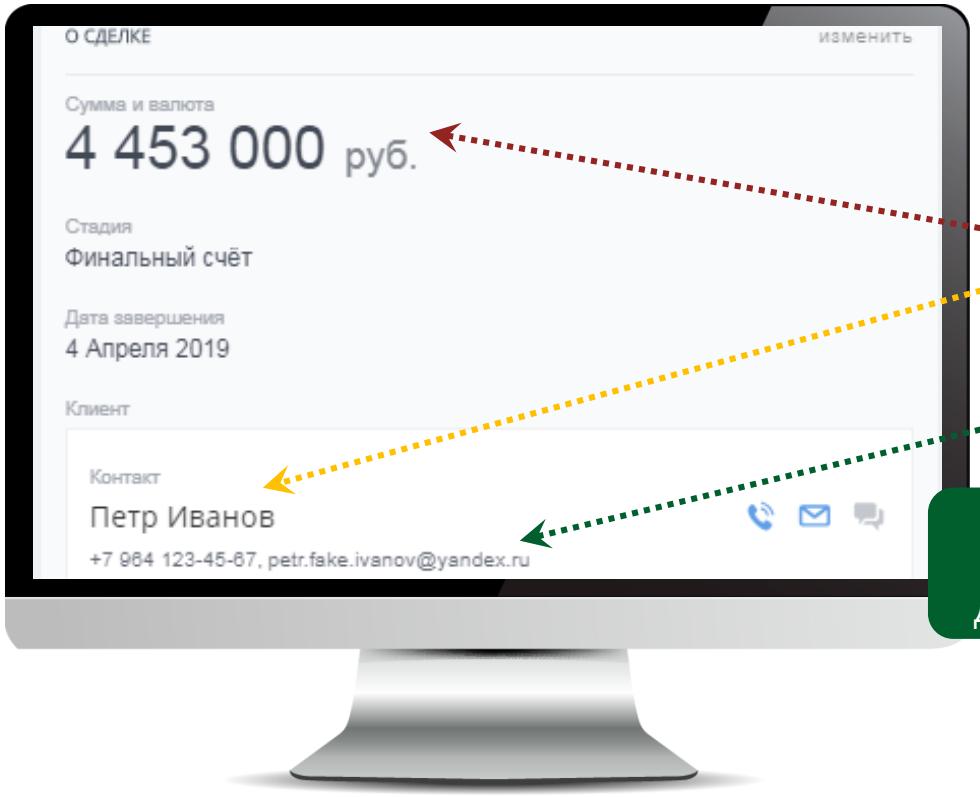
учет опечаток, транслитерации и морфологии

Более 120 словарей

включая наборы на других языках

Понимание специфики любой отрасли и создание словарей «под ключ»

Анализ



Simona	Morasca	3 502 2			
Mitsue	Tollner	3 749 1			
Leota	Dilliard	2 414 1			
Sage	Wieser	3 562 7			
Kris	Marrier	3 045 2			
Minna	Amigon	3 676 33			
Abel	Maclead	3 841 612	Rangoni Of Florence	631-335-3414	amacle
Kiley	Caldarera	3 593 615	Feiner Bros	310-498-5651	kiley.ca
Петр	Иванов	4 453 000	риз лицо	+7 964 123-45-67	petr.fa
Graciela	Ruta	4 808 288	Buckley Miller & Wright	440-780-8425	gruta@
Cammy	Albares	2 004 541	Rousseaux, Michael Esq	956-537-6195	calbare
Mattie	Poquette	3 158 495	Century Communications	602-277-4385	mattie(
Meaghan	Garufi	3 596 378	Bolton, Wilbur Esq	931-313-9635	meagha
Gladys	Rim	3 934 820	T M Byxbee Company Pc	414-661-9598	gladys.r
Yuki	Whobrey	4 895 322	Farmers Insurance Group	313-288-7937	yuki_w
Fletcher	Flosi	4 037 080	Post Box Services Plus	815-828-2147	fletche
			rt En Art	610-545-3615	bette_r
			Network Inc	408-540-1785	vinouye
			lls, Donald R Esq	972-303-9197	willard

Бланки

опросники, квитанции, анкеты и пр.

Выгрузки из БД

до 5 000 000 записей

Клиентские базы, финансовая информация, персональные данные и пр.

Анализ

карты

паспорта

Новые объекты

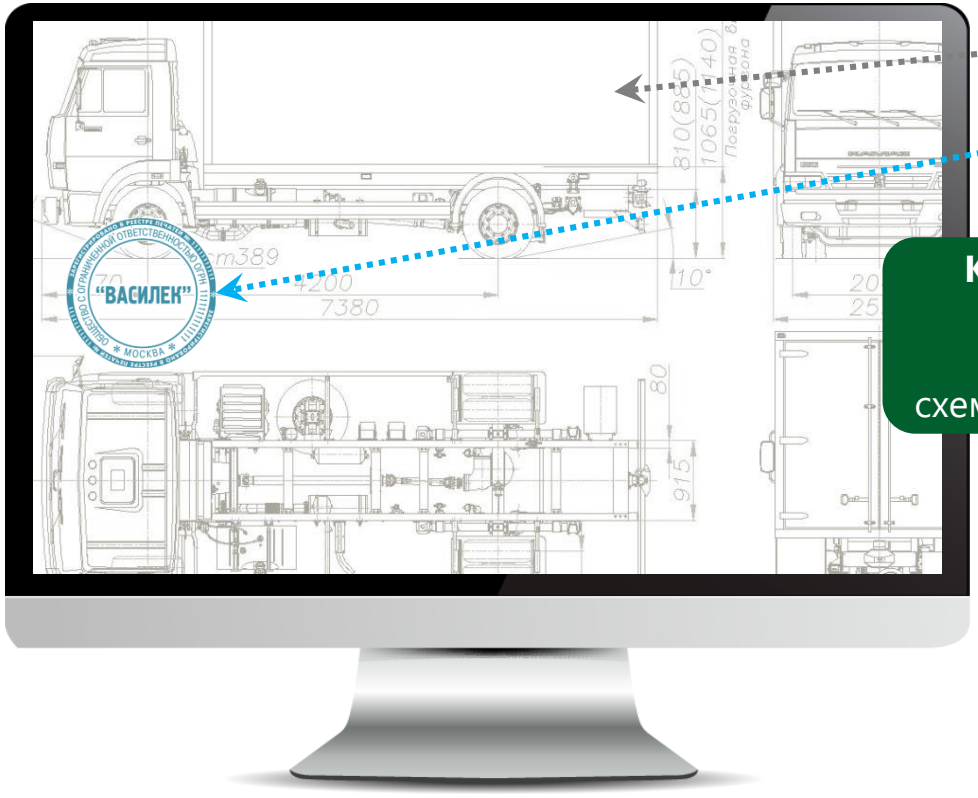
ID, водительские права и др.

Обученные детекторы

защита персональных данных

Готовые детекторы и возможность обучать систему

Анализ



отпечаток

печати

Защита векторной графики

Autodesk AutoCAD
и др.

Классификация объектов

схемы, карты, чертежи

Цифровые отпечатки

любые типы файлов

Растровая и векторная графика и любые другие файлы

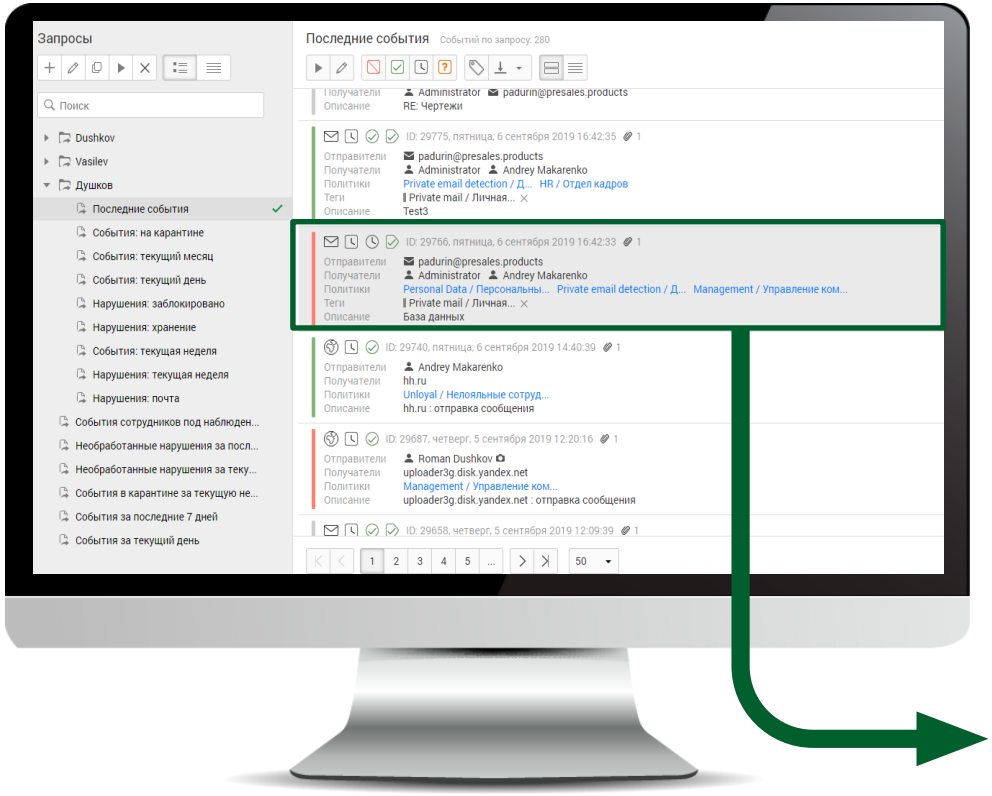
ШАГ 3: Решение

Автоматически или под управлением администратора система принимает **решения** по защите данных:

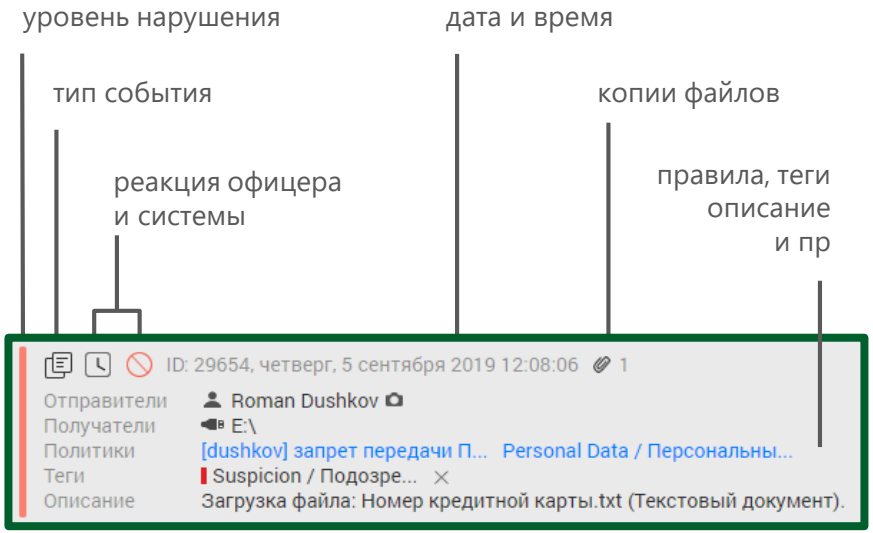
- Блокировка
- Карантин
- Разрешение

Автоматизация и экономия времени, блокировка и карантин

ШАГ 4: Хранение



Зоны видимости и поиск позволяют проводить **расследования** и **ретроспективный анализ**:



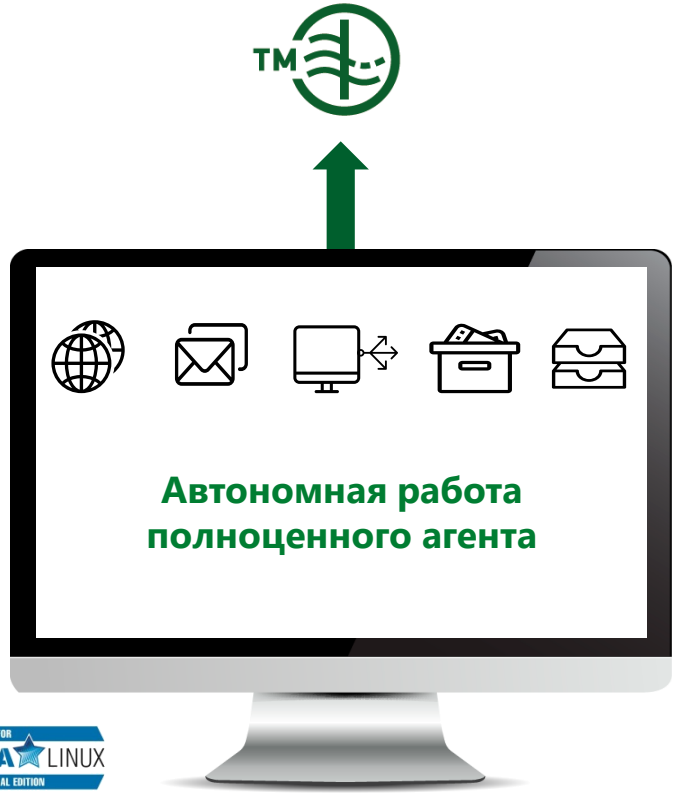
Инциденты можно анализировать в консоли либо выгружать в файлы

Агент на рабочих станциях

Сбор информации и срабатывание политик

Контроль доступа и блокировка

Работа как в открытом, так и в скрытом режимах

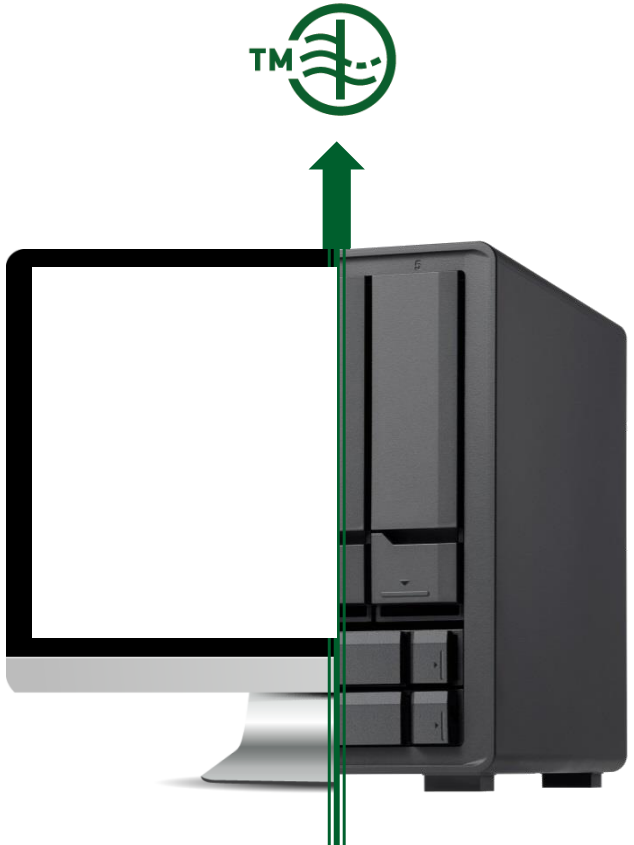


Сканер файлов покоя

Сканирование локальных и сетевых папок

Обнаружение нарушений правил хранения

Мониторинг без установки агентской части



Централизованный сбор данных

INFOWATCH®

Работа в режиме мониторинга и «в разрыв»

Защита корпоративной почты

Контроль на уровне proxy-серверов

INFOWATCH®

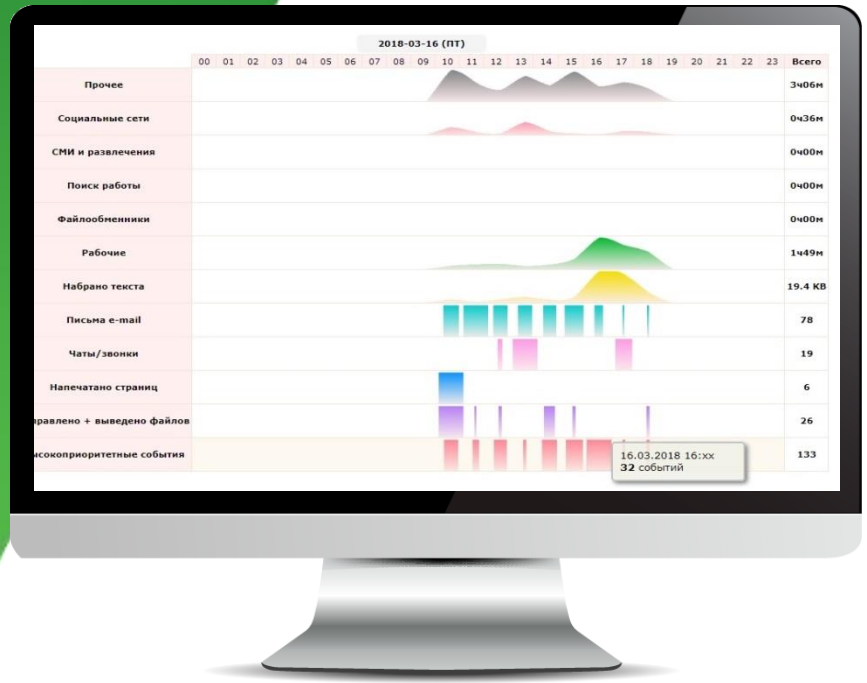
PERSON MONITOR

Точечный анализ

Анализирует рабочую активность сотрудника

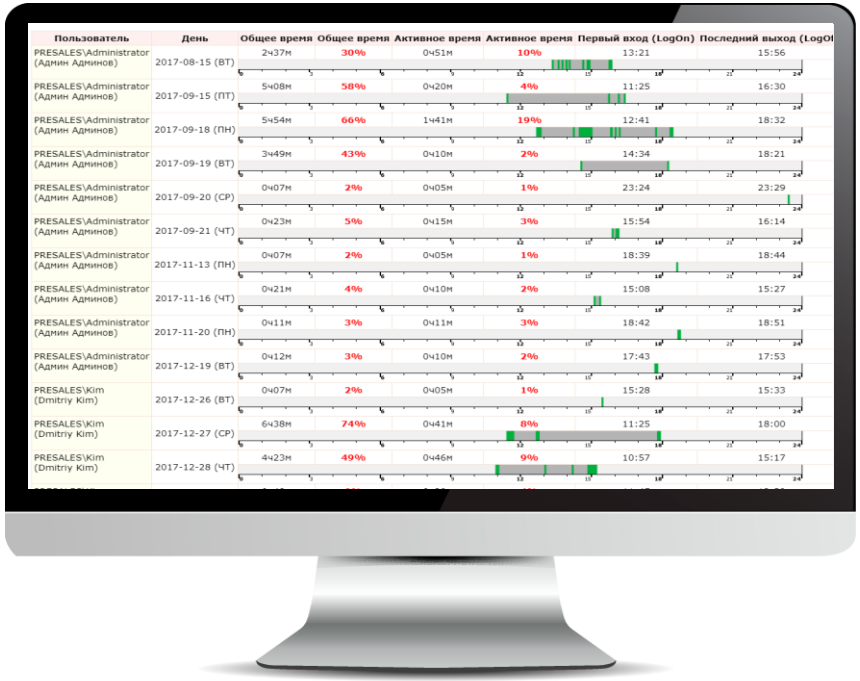
Помогает принимать решения

Помогает экономить на закупках

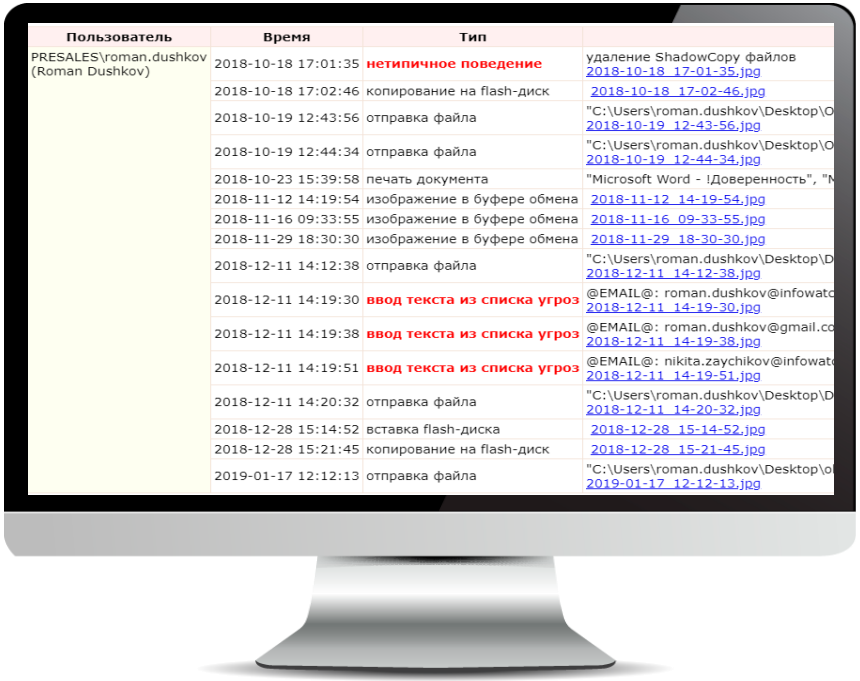


Точечный анализ

Десятки готовых отчетов отображают **картину рабочего дня** сотрудников



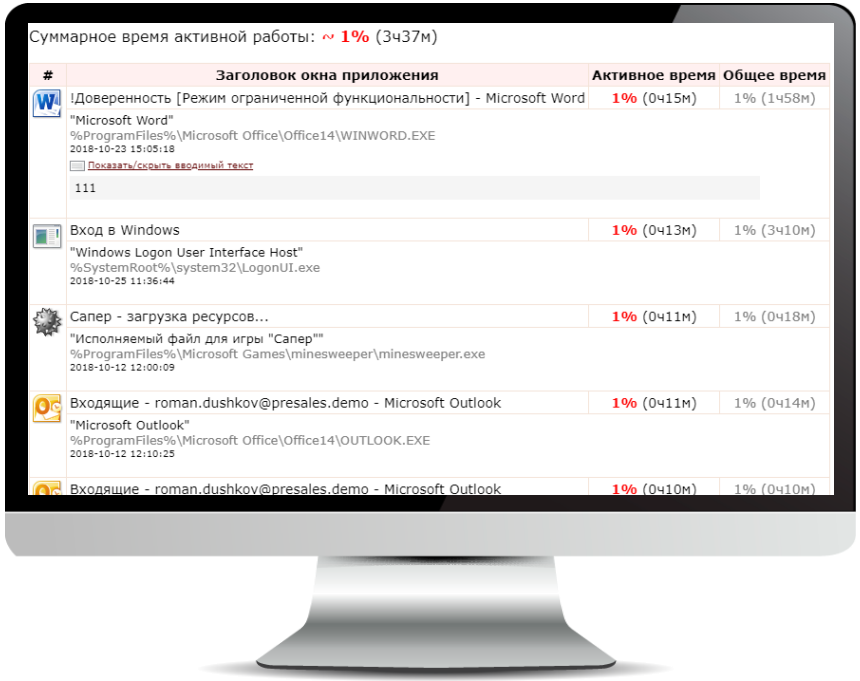
Пользователь	День	Общее время	Общее время	Активное время	Активное время	Первый вход (LogOn)	Последний выход (LogOf
PRESALES\Administrator (Админ Админов)	2017-08-15 (ВТ)	2ч37м	30%	0ч51м	10%	13:21	15:56
PRESALES\Administrator (Админ Админов)	2017-09-15 (ПТ)	5ч08м	58%	0ч20м	4%	11:25	16:30
PRESALES\Administrator (Админ Админов)	2017-09-18 (ПН)	5ч54м	66%	1ч41м	19%	12:41	18:32
PRESALES\Administrator (Админ Админов)	2017-09-19 (ВТ)	3ч49м	43%	0ч10м	2%	14:34	18:21
PRESALES\Administrator (Админ Админов)	2017-09-20 (СР)	0ч07м	2%	0ч05м	1%	23:24	23:29
PRESALES\Administrator (Админ Админов)	2017-09-21 (ЧТ)	0ч23м	5%	0ч15м	3%	15:54	16:14
PRESALES\Administrator (Админ Админов)	2017-11-13 (ПН)	0ч07м	2%	0ч05м	1%	18:39	18:44
PRESALES\Administrator (Админ Админов)	2017-11-16 (ЧТ)	0ч21м	4%	0ч10м	2%	15:08	15:27
PRESALES\Administrator (Админ Админов)	2017-11-20 (ПН)	0ч11м	3%	0ч11м	3%	18:42	18:51
PRESALES\Administrator (Админ Админов)	2017-12-19 (ВТ)	0ч12м	3%	0ч10м	2%	17:43	17:53
PRESALES\Kim (Dmitriy Kim)	2017-12-26 (ВТ)	0ч07м	2%	0ч05м	1%	15:28	15:33
PRESALES\Kim (Dmitriy Kim)	2017-12-27 (СР)	6ч38м	74%	0ч41м	8%	11:25	18:00
PRESALES\Kim (Dmitriy Kim)	2017-12-28 (ЧТ)	4ч23м	49%	0ч46м	9%	10:57	15:17



Пользователь	Время	Тип	
PRESALES\roman.dushkov (Roman Dushkov)	2018-10-18 17:01:35	нетипичное поведение	удаление ShadowCopy файлов 2018-10-18_17-01-35.jpg
	2018-10-18 17:02:46	копирование на flash-диск	2018-10-18_17-02-46.jpg
	2018-10-19 12:43:56	отправка файла	"C:\Users\roman.dushkov\Desktop\O 2018-10-19_12-43-56.jpg
	2018-10-19 12:44:34	отправка файла	"C:\Users\roman.dushkov\Desktop\O 2018-10-19_12-44-34.jpg
	2018-10-23 15:39:58	печать документа	"Microsoft Word - !Доверенность", "N
	2018-11-12 14:19:54	изображение в буфере обмена	2018-11-12_14-19-54.jpg
	2018-11-16 09:33:55	изображение в буфере обмена	2018-11-16_09-33-55.jpg
	2018-11-29 18:30:30	изображение в буфере обмена	2018-11-29_18-30-30.jpg
	2018-12-11 14:12:38	отправка файла	"C:\Users\roman.dushkov\Desktop\D 2018-12-11_14-12-38.jpg
	2018-12-11 14:19:30	ввод текста из списка угроз	@EMAIL@: roman.dushkov@infowatc 2018-12-11_14-19-30.jpg
	2018-12-11 14:19:38	ввод текста из списка угроз	@EMAIL@: roman.dushkov@gmail.co 2018-12-11_14-19-38.jpg
	2018-12-11 14:19:51	ввод текста из списка угроз	@EMAIL@: nikita.zaychikov@infowat 2018-12-11_14-19-51.jpg
	2018-12-11 14:20:32	отправка файла	"C:\Users\roman.dushkov\Desktop\D 2018-12-11_14-20-32.jpg
	2018-12-28 15:14:52	вставка flash-диска	2018-12-28_15-14-52.jpg
	2018-12-28 15:21:45	копирование на flash-диск	2018-12-28_15-21-45.jpg
	2019-01-17 12:12:13	отправка файла	"C:\Users\roman.dushkov\Desktop\o 2019-01-17_12-12-13.jpg

Точечный анализ

Работа в **программах** и **сайтах**, вводимый **текст** и возможные **риски**



INFOWATCH®

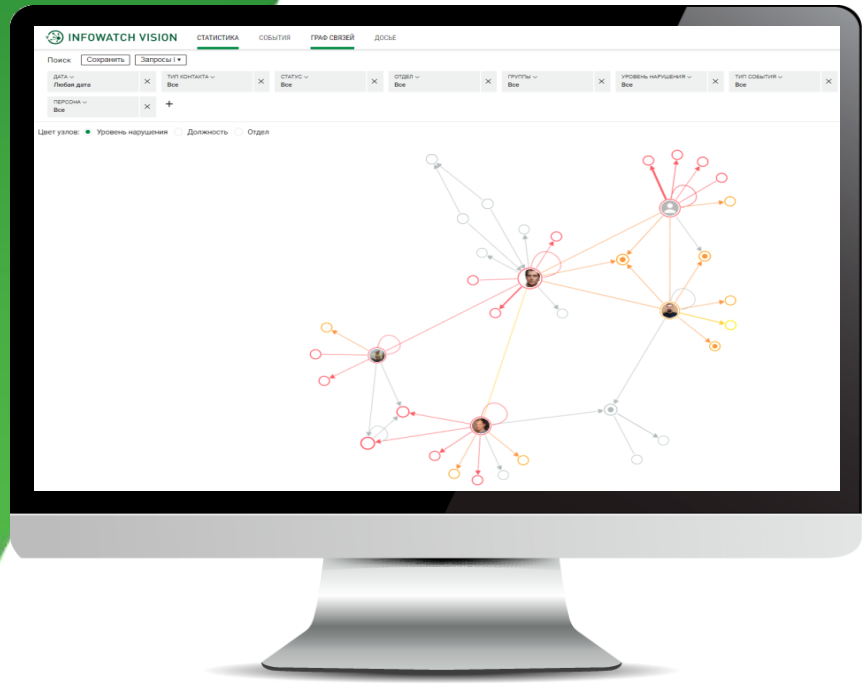
VISION

Визуализация инцидентов

Визуализирует связи сотрудников

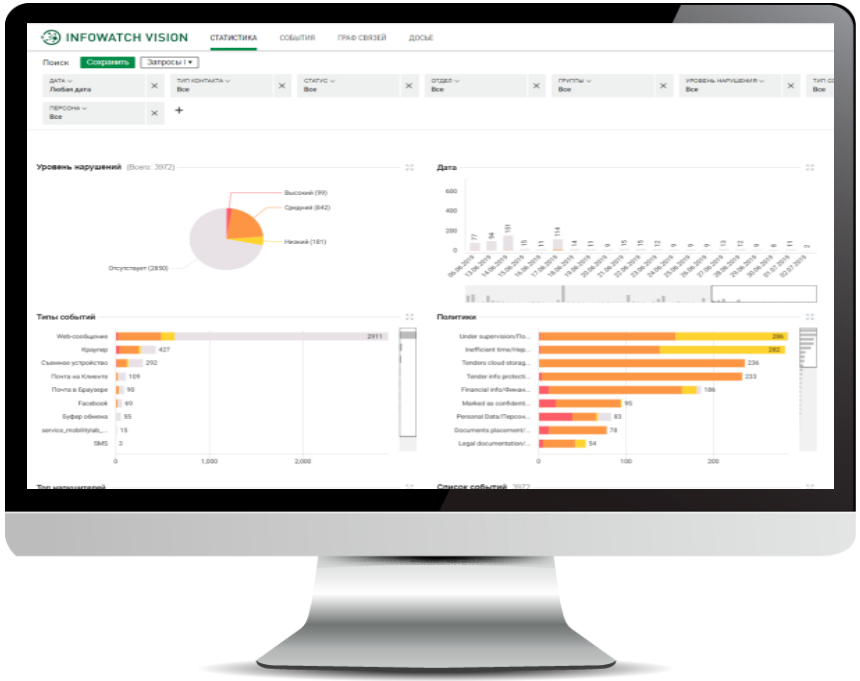
Обозначает аномальную активность

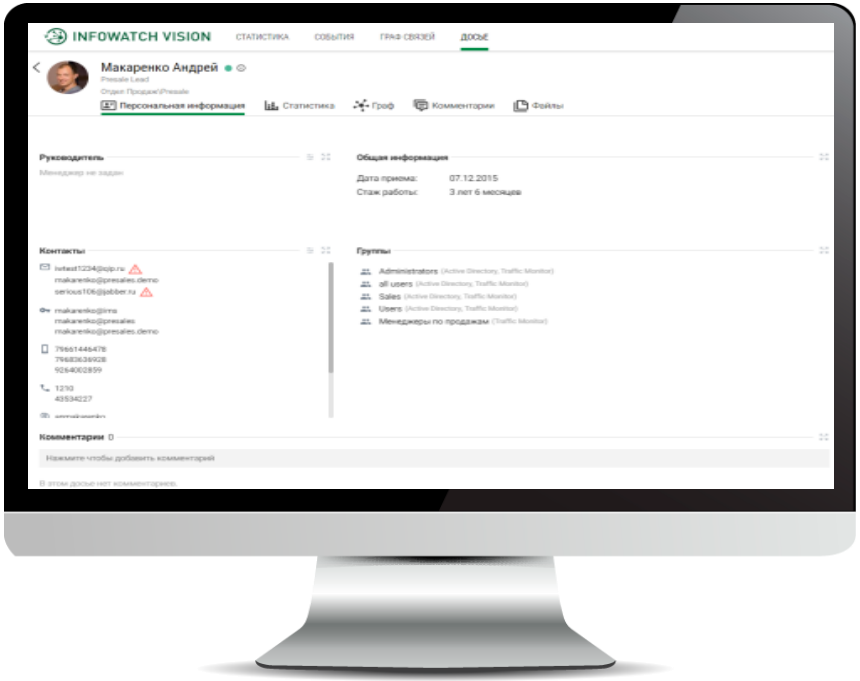
Позволяет быстро фильтровать события



Визуализация инцидентов

Все панели **связаны между собой** и отображают **единый срез данных**





Некоторые интеграции

INFOWATCH®

Exchange

SharePoint

WorksPad

ЦРТ

Office 365

SAP

ERP

Lync

ORACLE

ETHERSENSOR

Готовые проекты и SDK API для собственных разработок

Почему InfoWatch?

Сертифицированный продукт
продукты обладают необходимыми сертификатами и лицензиями (ФСБ, ФСТЭК)

Соответствие требованиям законодательства РФ
в области информационной безопасности, противодействию коррупции и защите персональных данных

Более двух тысяч успешно реализованных проектов
в организациях из различных областей экономики

Стаж, опыт и экспертиза
решения действительно работают на практике

INFOWATCH®

Всегда на связи

Высоцкий Павел
Менеджер по развитию бизнеса в ЦФО

Моб. +7 (960) 116-69-39
pavel.vysotskiy@infowatch.com