Расследование инцидентов информационной безопасности

Контур
staffcop

staffcop.ru

Возможности

- Мониторинг действий сотрудников
- Выявление инсайдерской деятельности
- Предотвращение утечек и сливов
- Выявление мошенничества и коррупции
- Оповещение о нарушении политик ИБ
- Блокировка нежелательной активности
- Расследование инцидентов

Резидент RUS®SOFT

Оглавление

О компании

Иван Хаустов,генеральный директор
ООО «АТОМ БЕЗОПАСНОСТЬ»

Staffcop (ООО «АТОМ БЕЗОПАСНОСТЬ», входит в группу компаний СКБ Контур) — один из лидеров в области разработки решений для обеспечения внутренней информационной безопасности.

Мы помогаем нашим клиентам защитить внутренний контур безопасности.

Команда экспертов Staffcop — это надёжный напарник, который поможет преодолеть любые сложности.

Наша задача не просто отвечать всем необходимым стандартам безопасности, но и подстраиваться под особенности бизнеса, без проблем интегрируясь в существующую ИТ и ИБ-инфраструктуру.

С нами можно сосредоточиться на развитии бизнеса и текущих задачах, не отвлекаясь на технические нюансы или риски несоответствия требованиям.

О компании

«АТОМ БЕЗОПАСНОСТЬ» — российская аккредитованная ИТ-компания, разработчик решений в области информационной безопасности.

Флагманский продукт компании Staffcop Enterprise — это софт, который помогает расследовать инциденты внутренней безопасности, восстанавливать хронологию событий, предотвращать утечки конфиденциальной информации, вести учёт рабочего времени и администрировать рабочие места.

Staffcop Enterprise сертифицирован ФСТЭК России, входит в реестр отечественного ПО.

«АТОМ БЕЗОПАСНОСТЬ» внесена в Единый реестр IT-компаний Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации с регистрационным номером 9965 запись № 95 от 15.03.2019 г. Staffcop Enterprise внесён в Единый реестр российского ПО под № 8828.

Сертификат ФСТЭК NQ4234. Соответствует требованиям документов: Требования к СКН, Профиль защиты СКН (контроля подключения съёмных машинных носителей информации четвёртого класса защиты. ИТ. СКН. П4. ПЗ), ЗБ.

13 лет
Экспертизы в информационной безопасности

3000
Клиентов в 40 странах мира

>250 тыс
ПК под защитой Staffcop

Лучшее ПО
По версии Forbes Advisor 2023 и 2024 года

Решаемые задачи

Информационная безопасность

- Расследование инцидентов внутренней информационной безопасности
- Выявление инсайдерской деятельности
- Выявление случаев мошенничества и коррупционных схем
- Поиск нелояльных сотрудников, выявление групп риска
- Предотвращение утечек и сливов чувствительной информации
- Своевременное оповещение о нарушении политик безопасности

Удалённое администрирование

- Расследование причин сбоев на рабочих станциях пользователей
- Выявление использования «нелегального» ПО
- Удалённое консультирование пользователей
- Защита локальной сети блокировкой USB-носителей
- Блокировка не относящихся к работе программ и сайтов

Повышение эффективности труда

- Контроль удалённых сотрудников и офисов
- Блокировка не относящихся к работе программ и сайтов
- Выявление сотрудников, желающих сменить место работы
- Выявление «узких» мест в бизнес-процессах
- Сравнение сотрудников/ отделов по ключевым показателям
- Контроль присутствия на рабочем месте

О Staffcop Enterprise

Система для расследования инцидентов внутренней информационной безопасности Staffcop Enterprise состоит из двух частей: сервера и службы-агента.

Агент запускается на рабочих станциях сотрудников или терминальных серверах, собирает критичные данные, фиксирует подозрительные события. Затем он передаёт информацию на сервер для хранения и обработки. Функционал сервера включает быстрый поиск, анализ и визуализацию данных.

Staffcop Enterprise может работать как в рамках локального закрытого периметра, так и на компьютерах, находящихся за его пределами.

Возможности

Расследования

Инцидентов внутренней информационной безопасности

Причин неэффективной работы и неправомерных действий сотрудников

Выявление

Коррупционных схем и мошенничества внутри компании

Нелояльных сотрудников, работающих на конкурентов

Уведомления

Регулярная рассылка отчетов по действиям и активности пользователей

Оповещение на почту или в Telegram по инцидентам безопасности

Блокировка

Копирования на съёмные носители

Пересылки конфиденциальной информации

Доступа к нерегламентированным ресурсам

Преимущества Staffcop Enterprise

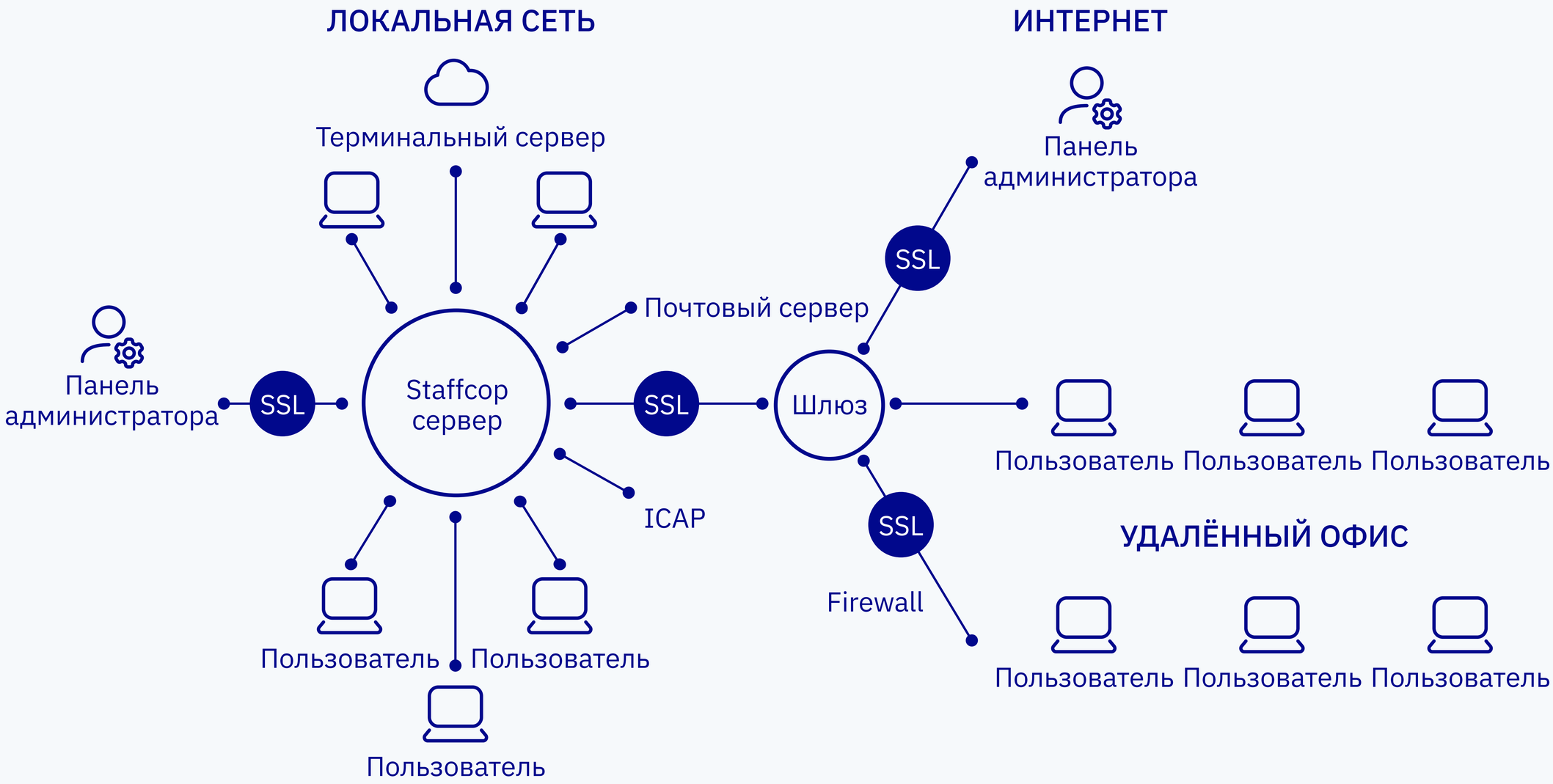
Плюсы сотрудничества

- Лёгкое внедрение в существующую инфраструктуру
- Индивидуальный подход, закреплённый менеджер
- Качественная и доступная техподдержка
- Расширенный тестовый период с полным функционалом
- Эффективная стоимость конечного владения
- Доступ к регулярным обновлениям

Преимущества продукта

- Сертифицирован ФСТЭК и ФСБ, входит в реестр отечественного ПО
- Быстрый и лёгкий
- Поддерживает различные ОС и ИБ-системы, открытое API
- Импортонезависимый и опенсорсный
- Работает в любых сетях
- Единый веб-интерфейс для управления
- Строит многомерные отчёты и выгружает аналитику
- Качественная и подробная документация

Архитектура



Работает в локальных, распределённых и смешанных сетях любой сложности

Особенности Staffcop

Единый веб-интерфейс

Взаимодействие с системой происходит через единый веб-интерфейс с гибким управлением, которое позволяет анализировать данные, устанавливать политики и реакции, настраивать работу системы и собирать статистику.

Горизонтально масштабируется

Staffcop Enterprise эффективно работает, как с несколькими компьютерами, так и с тысячами рабочих станций.

Современные технологии

В основе лежит OLAP — технология обработки данных для построения многомерных отчётов «на лету» и обработки больших объёмов данных за секунды.

Агент для Windows, Linux, macOS

Контроль ведётся на рабочих станциях, терминальных серверах, VDI. Агент работает на операционных системах Windows, Linux, macOS* функциональность агента на разных операционных системах отличается.

Особенности Staffcop

Для работы достаточно одного виртуального сервера

Сервер работает на операционной системе Linux (Astra, Ubuntu) и может быть установлен как на физической, так и на виртуальной машине.

Локальное хранение

Агент без доступа к серверу полноценно функционирует: собирает данные в локальную базу данных и ограничивает действия пользователь: блокирует доступ к каналам передачи данных и утечки.

Возможности интеграции

- Открытое API
- Получение данных об отсутствии из 1С
- Получение данных от СКУД
- Передача данных в SIEM посредством Syslog

Минимальные требования к инфраструктуре

Минимальные требования к серверу:
100 пк <=> 6 СИ, 32 RAM. 1000 пк <=> 14 СИ, 96 RAM.

Минимальная нагрузка от агента для данного класса решений.

Как работает?

Сбор данных

Агент собирает все необходимые данные специалистам для расследования и передаёт их на сервер. Сервер обрабатывает полученную информацию, что позволяет использовать её для анализа, оповещения

Анализ

Визуальный и статистический анализ данных для выявления отклонений в поведении пользователей, поиска инцидентов, инсайдеров и нелояльных сотрудников.

Поиск

- Поиск информации в любых событиях на основе морфологии, фраз и регулярных выражений.
- Поиск похожих документов, печатей и паспортов, анализ ближайших событий и снимков экрана.

Как работает?

Расследование

– Управление расследованиями через систему: организация, контроль и запись действий в ходе расследования, назначение ответственных и отметка фигурантов, работа на основе приоритетов и фильтров.

– Возможность перехода из отчётов и графического анализа к конкретным событиям позволяет находить данные, очищенные от информационного шума, в несколько кликов.

Оповещение

Автоматическое оповещение отправленное на почту или в мессенджер о нарушении политики безопасности, опасной, аномальной и непродуктивной деятельности сотрудников.

Блокировка

– Операций с файлами на основе содержимого, меток и атрибутов (пути, форматы, тип контента).

– Доступа к съёмным носителям, полная или только для чтения.

– По классам и группам устройств, на основе чёрных и белых списков.

– Запуска приложений и доступа к сайтам, использование Wi-Fi сети.

Возможности интеграции

Открытый API и передача данных через Syslog позволяет дополнять данными для комплексного анализа и обработки инцидентов.

Возможность дополнять профиль пользователя данными с помощью синхронизации с Active Directory. Группировка и анализ данных по отделам, формирование отчётов для руководителей.

Контроль и анализ рабочих коммуникаций и передачу данных через почтовый сервер IMAP.

Для комплексного анализа рабочего дня сотрудников система позволяет дополнять расписание данными табеля отсутствия из 1С.

Получение данных сетевого трафика со стороны шлюзового решения посредством интеграции на основе ICAP-протокола.

Для проведения анализа нахождения сотрудников на рабочем месте реализована интеграция со СКУД.

Как Staffcop взаимодействует с другими решениями

Защита ваших филиалов

DLP более надёжно контролирует сетевой трафик на шлюзе. Staffcop контролирует действия пользователей на рабочих станциях.
При этом системы друг с другом не конфликтуют.

Эшелонированная защита

Увеличение надёжности защиты при нескольких решениях по ИБ.

На одной группе риска DLP. На другой — Staffcop

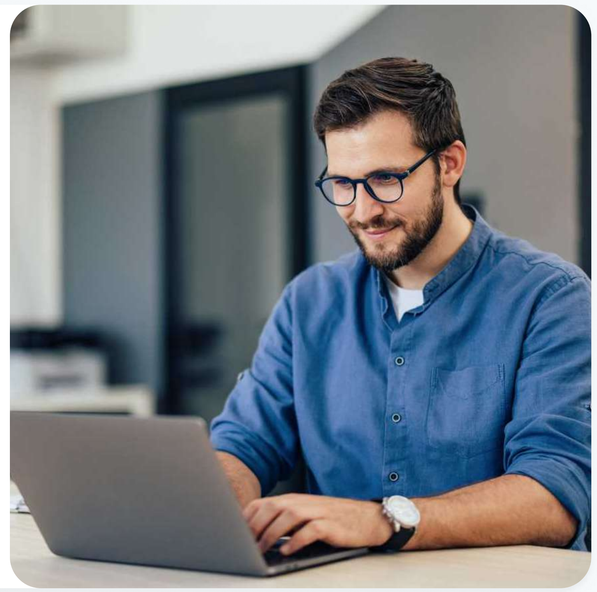
DLP контролирует одну группу риска внутренней информационной безопасности, Staffcop Enterprise контролирует действия пользователей и обнаруживает аномалии.

Оптимизация бюджета защиты ИБ

Если DLP защищает центральный офис, то на филиалах можно установить дополнительную защиту.

Staffcop Enterprise, как дополнение

Система предоставляет инструментарий для помощи администраторам. В реальном времени можно не только удалённо подключиться к рабочей станции пользователя, для анализа проблем или детального изучения аномальной активности пользователя, но и получить доступ к управлению станцией.



Использование отечественного и независимого ПО

Технологии сервера:
компоненты, не требующие лицензирования и покупки

ASTRA LINUX® · open source initiative · ClickHouse · Jatoba · PostgreSQL · NGINX

Доказано совместимы с:

ASTRA LINUX® · РЕДОС · SIEM · ROSA · base alt · Ankey ASAP · AlterOS

Подходит
для импортозамещения:

- Сертификат ФСТЭК
- Работает на открытом ПО, защищён от санкций
- Входит в реестр отечественного ПО
- СУБД: PostgreSQL, ClickHouse, Jatoba
- Сервер на Ubuntu и Astra Linux

Основные функции

- Действия пользователей
- Сетевой трафик
- Документы и файлы
- Контроль АРМ

staffcop.ru

Действия пользователей

Учёт рабочего времени

Мониторинг активности пользователя ПК. Интеграция со СКУД. Категоризация активности на продуктивную и непродуктивную.

Снимки экрана и видеозапись рабочего стола

Обогащение данных по действиям пользователя за счёт информации на экране сотрудника.

Контроль пользовательской активности

Контроль пользовательской сессии, локальной и удалённой, логирование входа и выхода из системы. Контроль опозданий и ранних уходов.

Контроль ввода данных

Контроль информации при вводе данных с клавиатуры и копировании в буфер обмена.

Мониторинг бизнес-процессов

Поиск узких мест, выявление блокирующих факторов и расследование причин их появления. Анализ бизнес-процессов по KPI.

Запись аудио с микрофона и снимки с веб-камер

Контроль окружающего пространства рабочего места сотрудника. Идентификация сотрудника на основе распознавания лиц.

Документы и файлы

Контроль почтовой переписки

Контроль переписки и передачи файлов через почтовые сервисы по протоколам POP3, IMAP, SMTP, MAPI.

Перехват переписки напрямую с корпоративногопочтового сервера.

Контроль устройств

Фиксация времени подключения и отключения, перехват файлов при загрузке на устройства хранения и на самом устройстве.

Блокировка по типам и параметрам устройств, чёрным и белым спискам.

Контроль печати

Отслеживание файлов во время отправки на печать.

Контроль количества страниц и времени отправки, теневых копий файлов.

Файловый сканер

Анализ содержимого и атрибутов файлов.

Поиск конфиденциальной информации на рабочих станциях сотрудников.

Контроль файловых операций

Контроль файловых операций.

Блокировка доступа перемещения и изменения файлов с конфиденциальной информацией.

Сетевой трафик

Перехват сообщений в корпоративных мессенджерах

Контроль внутренней переписки в мессенджерах: MS Teams, Vk Teams, Express, Bitrix24. Анализ переписки для выявления неправомерных действий сотрудников.

Перехват сообщений в некорпоративных мессенджерах

Фиксация содержимого, вложенных файлов и времени отправки или получения сообщения в WhatsApp, Telegram, Skype. Контролируйте передачу конфиденциальной информации.

Контроль использования веб-ресурсов

- Мониторинг сайтов
- Контроль активности в социальных сетях
- Перехват поисковых запросов
- Блокировки доступа к веб-ресурсам

Контроль облачных ресурсов

Контролируйте данные, которые передаются посредством корпоративных и публичных облачных сервисов хранения информации.

Контроль АРМ

Контроль Wi-Fi

Возможность полноценно ограничить нерегламентированный доступ в интернет.

Удаленное администрирование

Перехват управления и блокировка рабочей сессии. Удаленный просмотр до 16 рабочих столов одновременно.

Инвентаризация компьютеров

Полный список программных продуктов и аппаратного обеспечения на рабочем ПК.

Блокировка приложений

Блокировка запуска нерегламентированных, запрещенных и опасных программных продуктов.

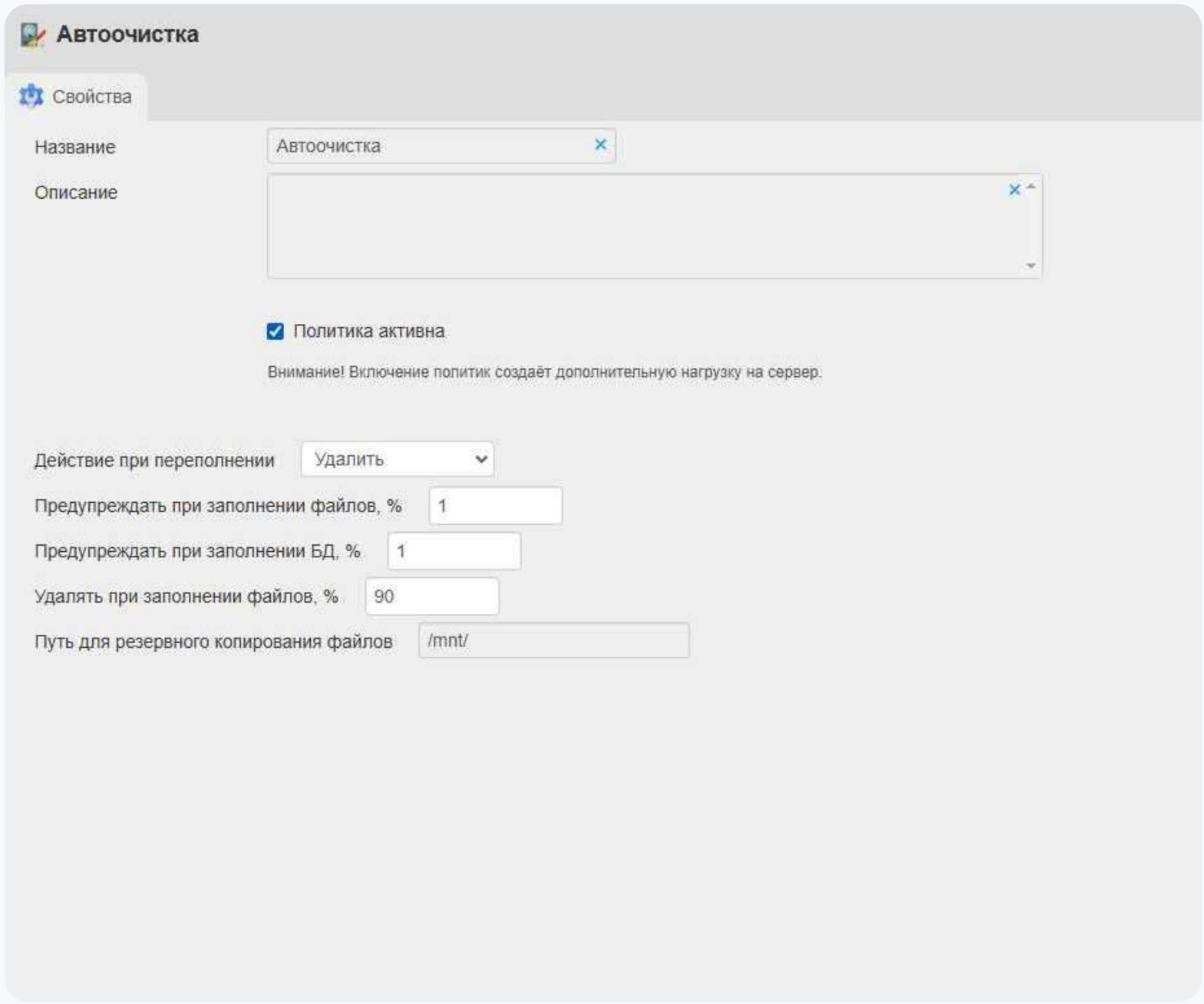
Ключевые нововведения Staffcop 5.5

- Анализ рисков
- Централизованное сканирование и установка меток
- Развитие функционала пакетов снимков экрана
- Перехват командной строки
- Перехват файлов, передаваемых через RDP
- Расширение функционала агентов для MacOS и Linux
- Учёт активности в ВКС
- Новый интерфейс

staffcop.ru

Архив данных

Система позволяет точно выбирать, какие данные и в каком объёме хранить в архиве.
это помогает оптимально использовать свободное место без ущерба задачам.

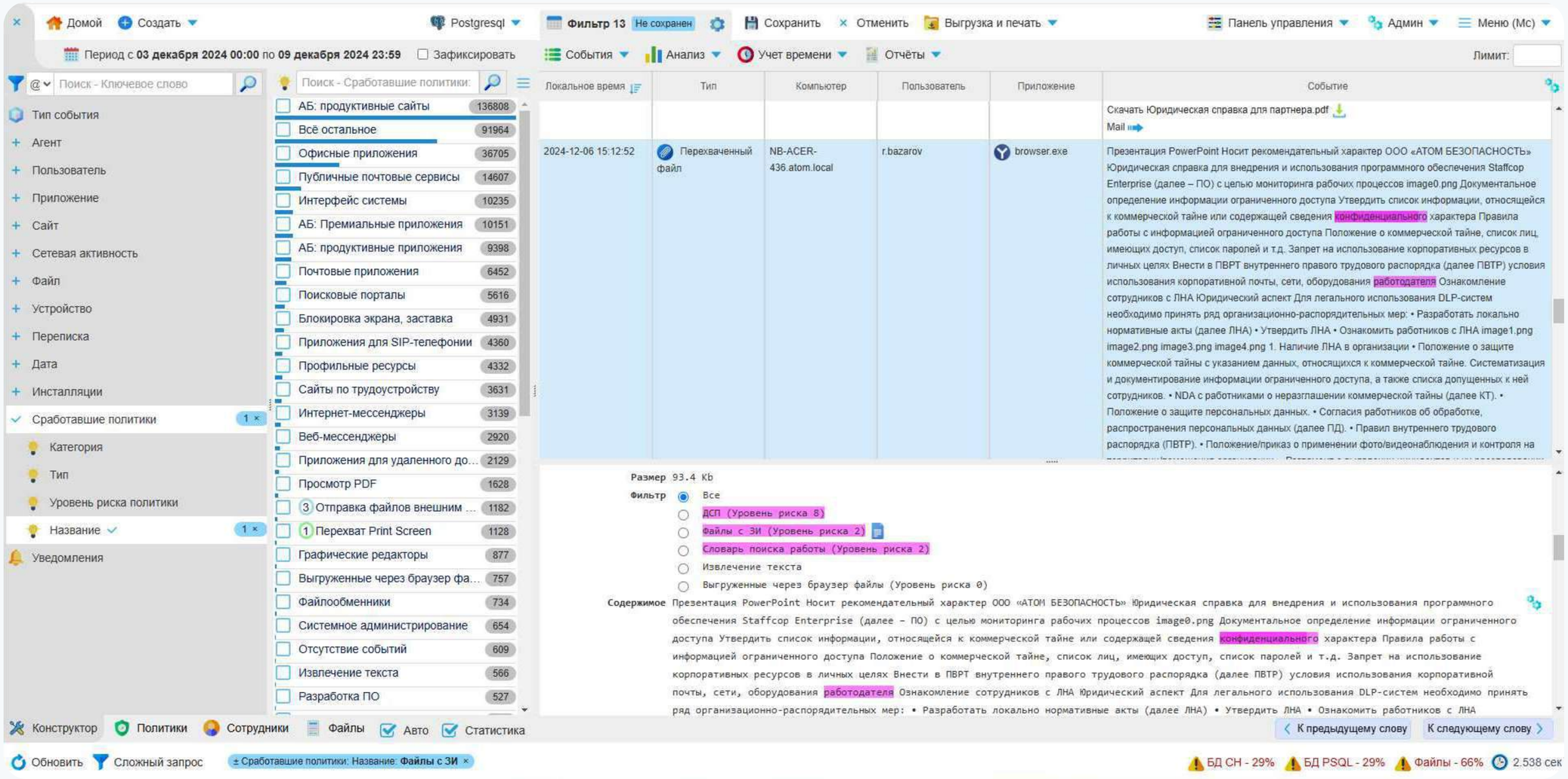


Поиск по словам и регулярным выражениям

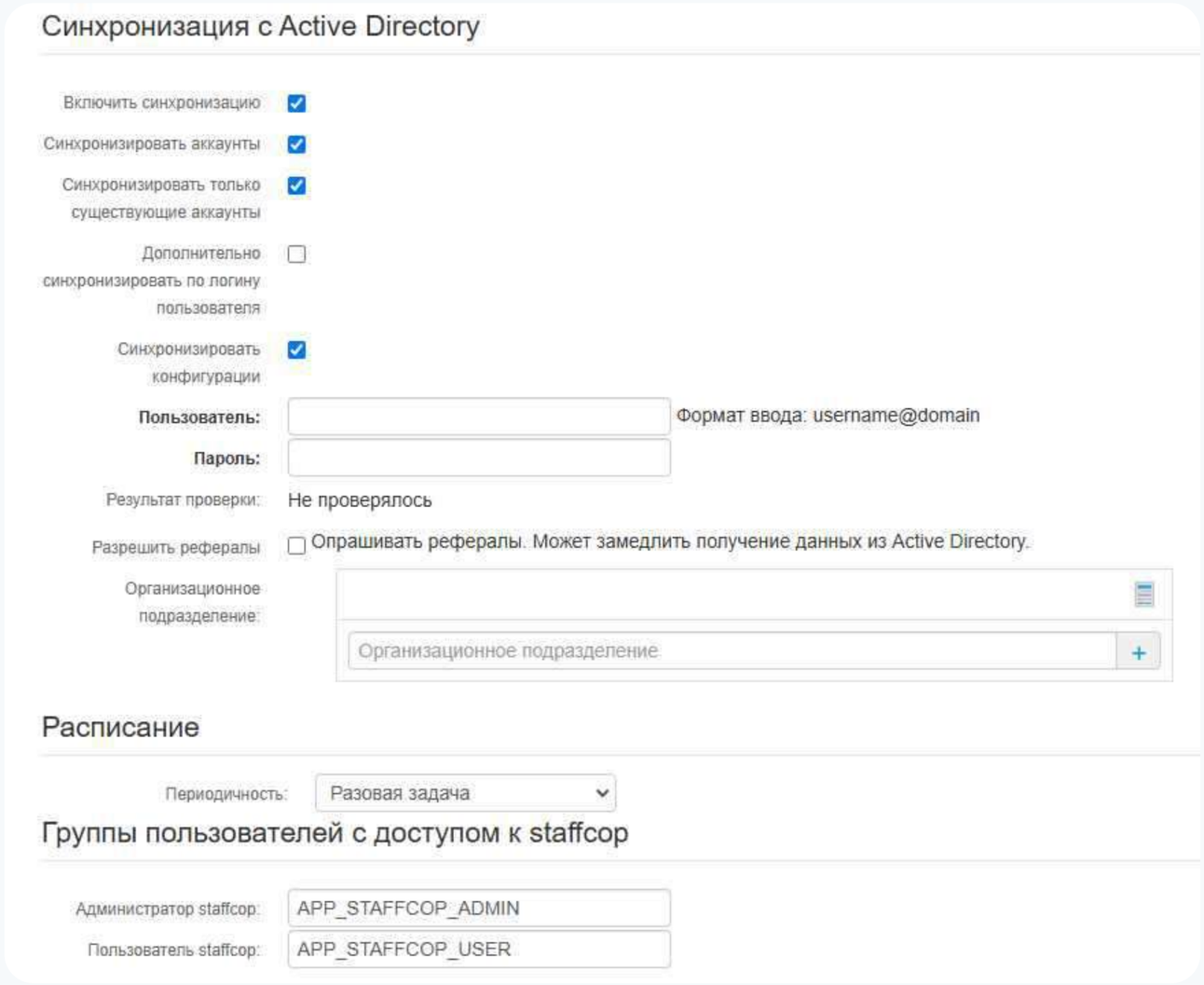
Выявляйте инциденты в передаваемых данных и действиях сотрудников с помощью слов-триггеров. Система позволяет настроить словари с реакцией не только на количество триггерный слов и выражений, но и учитывать общее содержание и атрибуты события.

Это позволяет обнаружить утечку данных, получить представление о сотрудниках и предотвратить проблемы.

Регулярные выражения точно выявляют передачу структурированной информации, такой как личные данные, конфиденциальные документы и служебная информация.



Синхронизация данных с AD



При синхронизации данных с Active Directory система обогащается информацией о профилях пользователей. это позволяет выявлять инциденты, создавать политики безопасности и продуктивности. Например, можно открыть доступ к сайтам по трудоустройству для отдела кадров и уведомлять администратора о получении конфиденциальных документов сотрудниками на испытательном сроке.

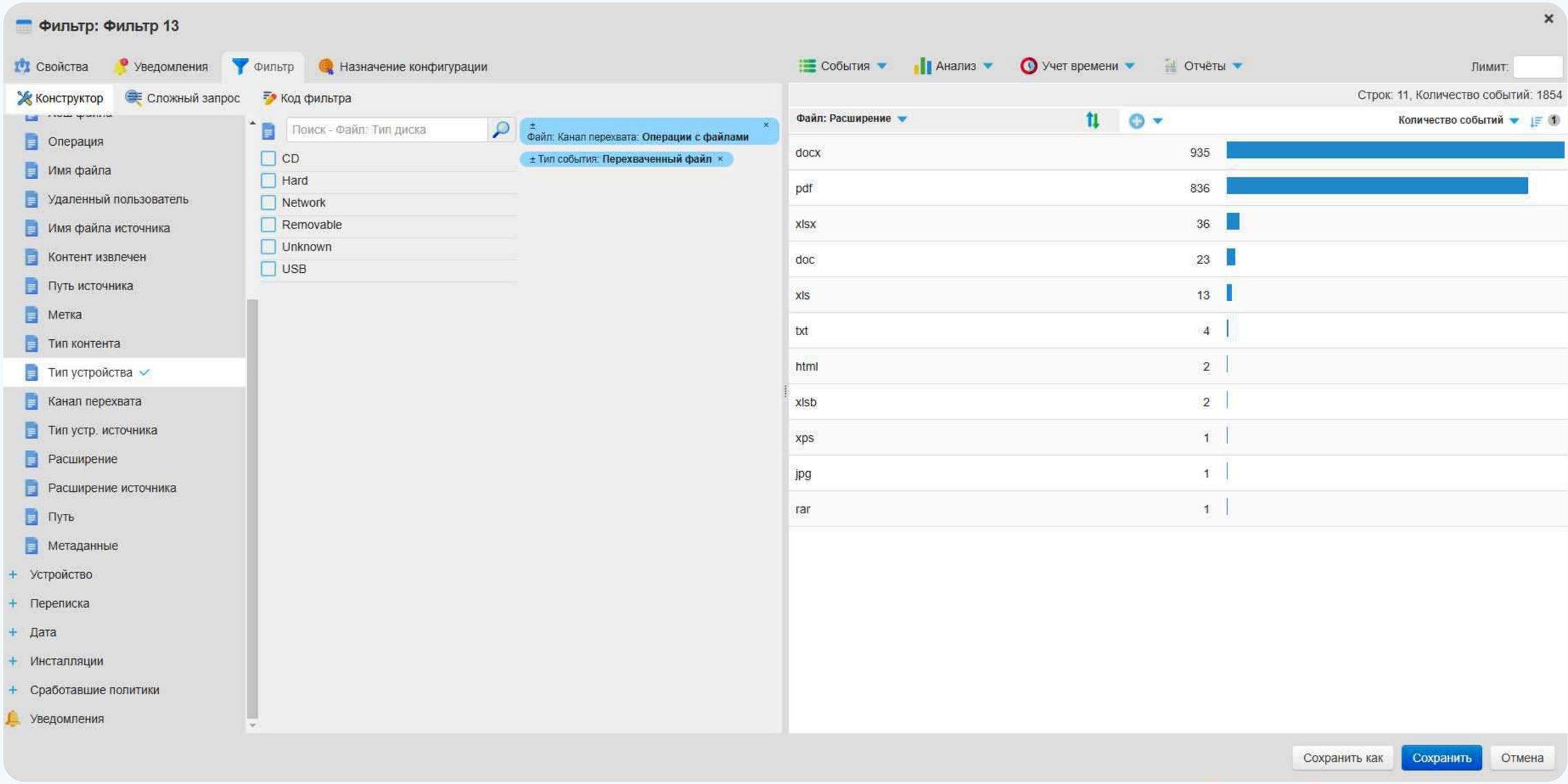
Для предоставления доступа пользователям к отчётам по самому себе — добавьте их в группу «Пользователи», для доступа Руководителям к данным по их подразделениям — настройте необходимые права доступа и добавьте руководителей в кастомную группу с настроенными правами доступа.

Гибкий и интерактивный конструктор отчётов и фильтров

Для поиска и анализа информации используется приём последовательного наложения ограничивающих фильтров. Наложение каждого фильтра в режиме реального времени отсекает лишнюю информацию, что позволяет находить данные в 2–3 клика.

Выбирайте форму и содержимое визуализации выбранных данных. Сохраняйте и используйте настроенные фильтры, чтобы не собирать нужные отчёты заново.

Также можно настроить в отчётах отправку уведомлений при появлении новых событий или отправку отчёта по новым событиям за период.



Множество графиков и диаграмм

Сводные отчёты в простом и удобном виде в рамках одного окна отображают самые важные характеристики и связанные события для выбранного объекта. Карточки сотрудников позволяют быстро получать агрегированную информацию по работнику, выявлять аномалии в активности и действиях, переводить сотрудника на особый контроль. Комплексный профиль содержит большой объём необходимой статистической информации по сотруднику.

Учёт рабочего времени за период с 3 декабря 2024 по 9 декабря 2024

Антипов Петр Евгеньевич

Сотрудник 1	Начало		Окончание		Общее время		Дисциплина		Активность		Продуктивность		
07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
3 декабря 2024 г.	9ч 51м 31с	9ч 00м 00с	19ч 00м 21с	20ч 00м 00с	9ч 08м 50с	8ч 00м 00с	1ч 08м 50с	51м 31с	7ч 36м 59с	1ч 31м 51с	5ч 07м 20с	48с	31м 33с
4 декабря 2024 г.	9ч 54м 42с	9ч 00м 00с	19ч 00м 56с	20ч 00м 00с	9ч 06м 14с	8ч 00м 00с	1ч 06м 14с	54м 42с	7ч 25м 10с	1ч 41м 04с	3ч 27м 06с	00с	09м 06с
5 декабря 2024 г.	9ч 45м 22с	9ч 00м 00с	19ч 28м 26с	20ч 00м 00с	9ч 43м 04с	8ч 00м 00с	1ч 43м 04с	45м 22с	7ч 08м 55с	2ч 34м 09с	4ч 45м 49с	00с	04м 03с
6 декабря 2024 г.	9ч 59м 38с	9ч 00м 00с	19ч 00м 10с	20ч 00м 00с	9ч 00м 32с	8ч 00м 00с	1ч 00м 32с	59м 38с	7ч 43м 06с	1ч 17м 26с	6ч 50м 14с	00с	09м 45с
8 декабря 2024 г.	9ч 59м 30с	нераб.	19ч 00м 07с	нераб.	9ч 00м 37с	00с	9ч 00м 37с	00с	6ч 23м 08с	2ч 37м 29с	5ч 31м 36с	00с	01м 13с
9 декабря 2024 г.	9ч 58м 20с	9ч 00м 00с	14ч 27м 20с	20ч 00м 00с	4ч 29м 00с	8ч 00м 00с	00с	58м 20с	2ч 49м 55с	1ч 39м 05с	2ч 19м 34с	00с	01м 38с

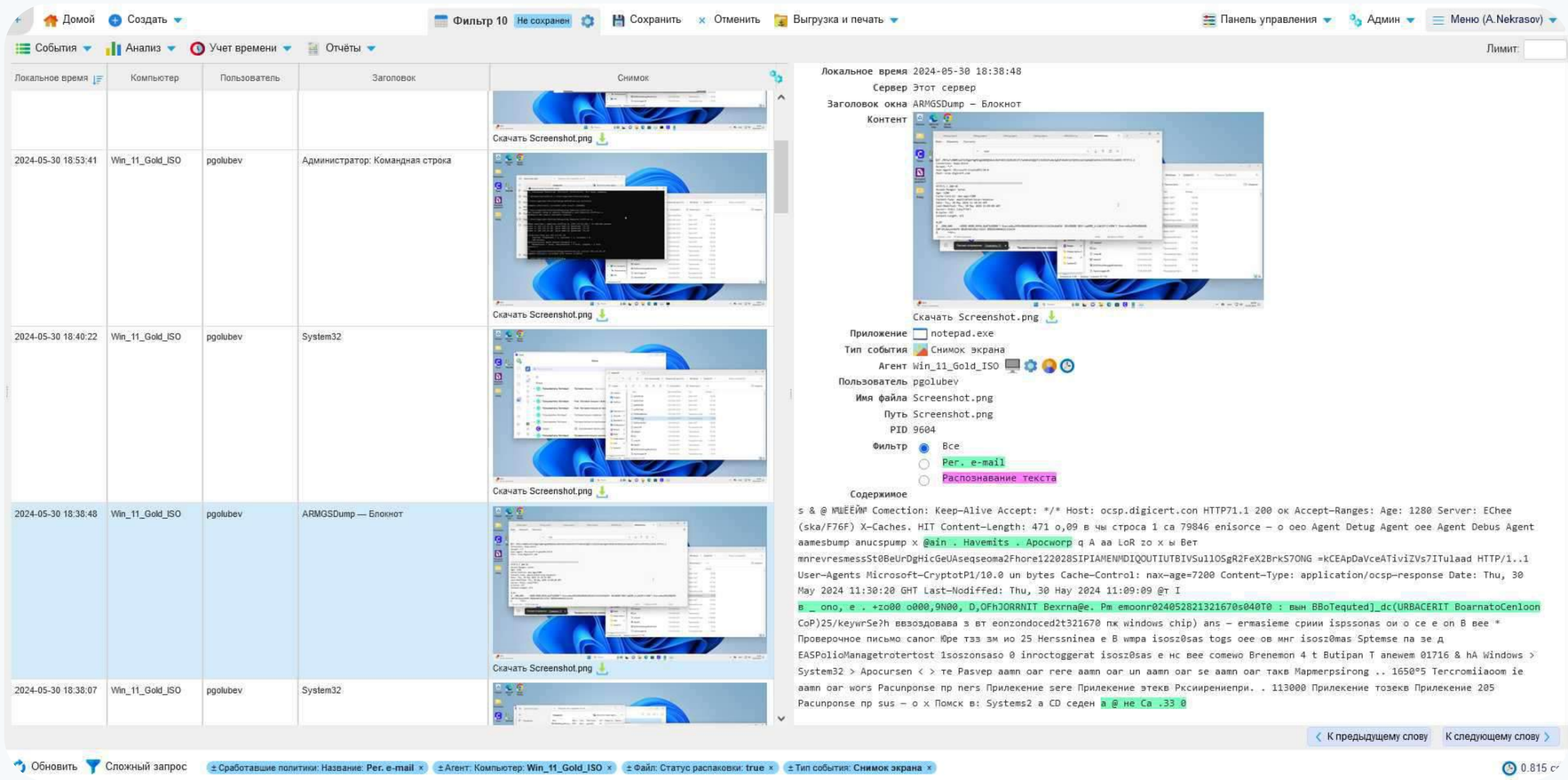
Антонов Владимир Сергеевич

Сотрудник 2 Дата	Начало		Окончание		Общее время		Дисциплина		Активность		Продуктивность		
00 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23	факт	распис	факт	распис	факт	план	сверх	опозд	актив	неактив	прод	непрод	нейтр
3 декабря 2024 г.	9ч 29м 49с	9ч 00м 00с	18ч 35м 12с	20ч 00м 00с	9ч 05м 23с	8ч 00м 00с	1ч 05м 23с	29м 49с	5ч 12м 28с	3ч 52м 55с	3ч 13м 37с	00с	20м 28с
4 декабря 2024 г.	9ч 54м 41с	9ч 00м 00с	18ч 10м 47с	20ч 00м 00с	8ч 16м 06с	8ч 00м 00с	16м 06с	54м 41с	5ч 39м 54с	2ч 36м 12с	3ч 28м 42с	42м 27с	17м 44с
5 декабря 2024 г.	9ч 45м 24с	9ч 00м 00с	17ч 43м 13с	20ч 00м 00с	7ч 57м 49с	8ч 00м 00с	00с	45м 24с	4ч 24м 00с	3ч 33м 49с	2ч 36м 08с	00с	10м 30с
6 декабря 2024 г.	9ч 44м 10с	9ч 00м 00с	17ч 48м 06с	20ч 00м 00с	8ч 03м 56с	8ч 00м 00с	03м 56с	44м 10с	3ч 11м 48с	4ч 52м 08с	1ч 46м 40с	13с	12м 07с
9 декабря 2024 г.	9ч 41м 52с	9ч 00м 00с	14ч 27м 00с	20ч 00м 00с	4ч 45м 08с	8ч 00м 00с	00с	41м 52с	2ч 52м 39с	1ч 52м 29с	2ч 03м 37с	00с	09м 22с

Распознавание текста в графическом и аудиоконтенте

Передаваемая информация содержится не только в текстовых файлах. Зачастую это могут быть сканы документов, графики или чертежи. Система извлекает и анализирует текстовую информацию из таких документов. Можно распознать и снимки рабочего стола сотрудника, чтобы превентивно определить, что сотрудник получил доступ к нерегламентированной информации до того, как решил её передать.

Распознавание аудиоконтента позволяет обнаруживать мошеннические действия и расследовать конфликты сотрудников за счёт анализа аудиотрафика с микрофона рабочей станции.



Расследование инцидентов ИБ

При сборе больших объёмов информации важно оперативно реагировать на обнаружение инцидентов. Система позволяет настроить отправку уведомлений специалисту на почту или в Telegram при обнаружении действия сотрудника, требующего особого внимания. она также позволяет регулярно отправлять отчёты с агрегированными данными для анализа действий сотрудников.

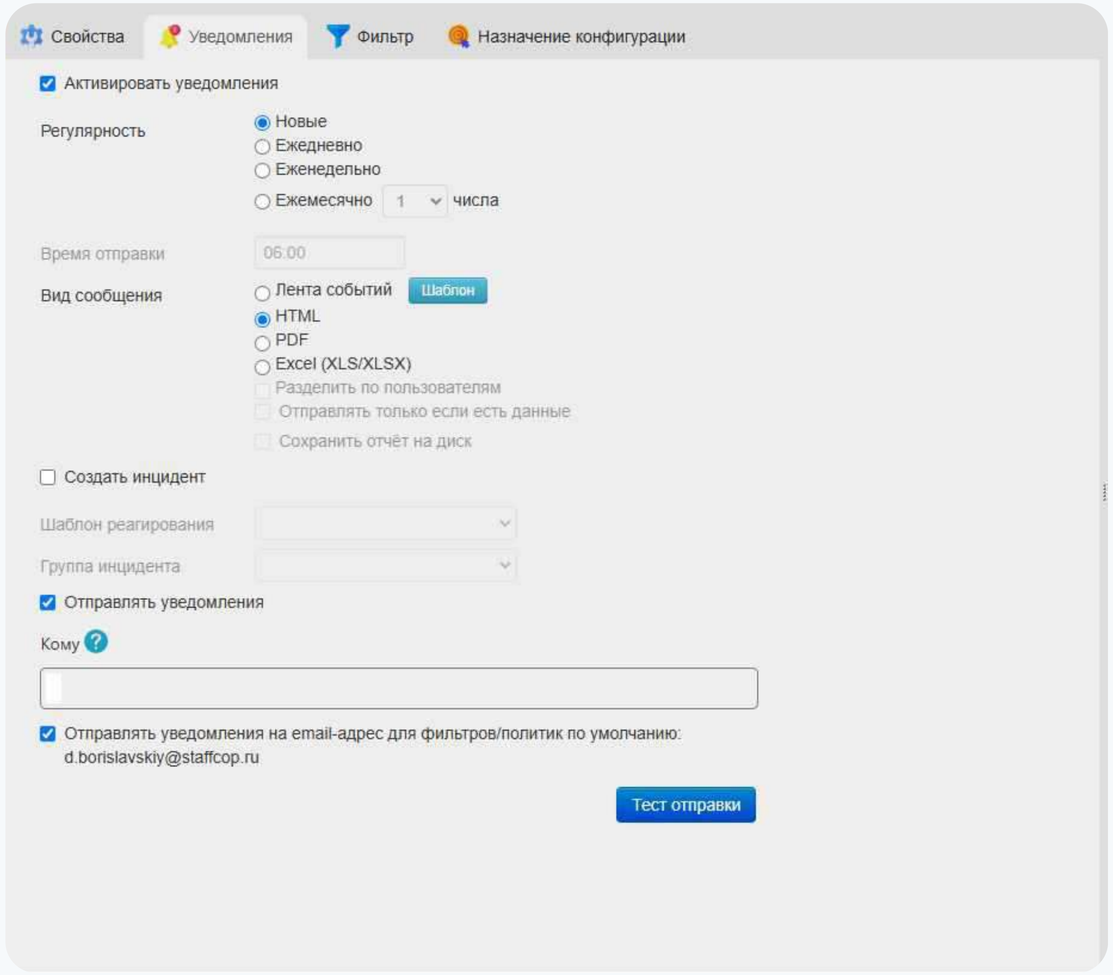
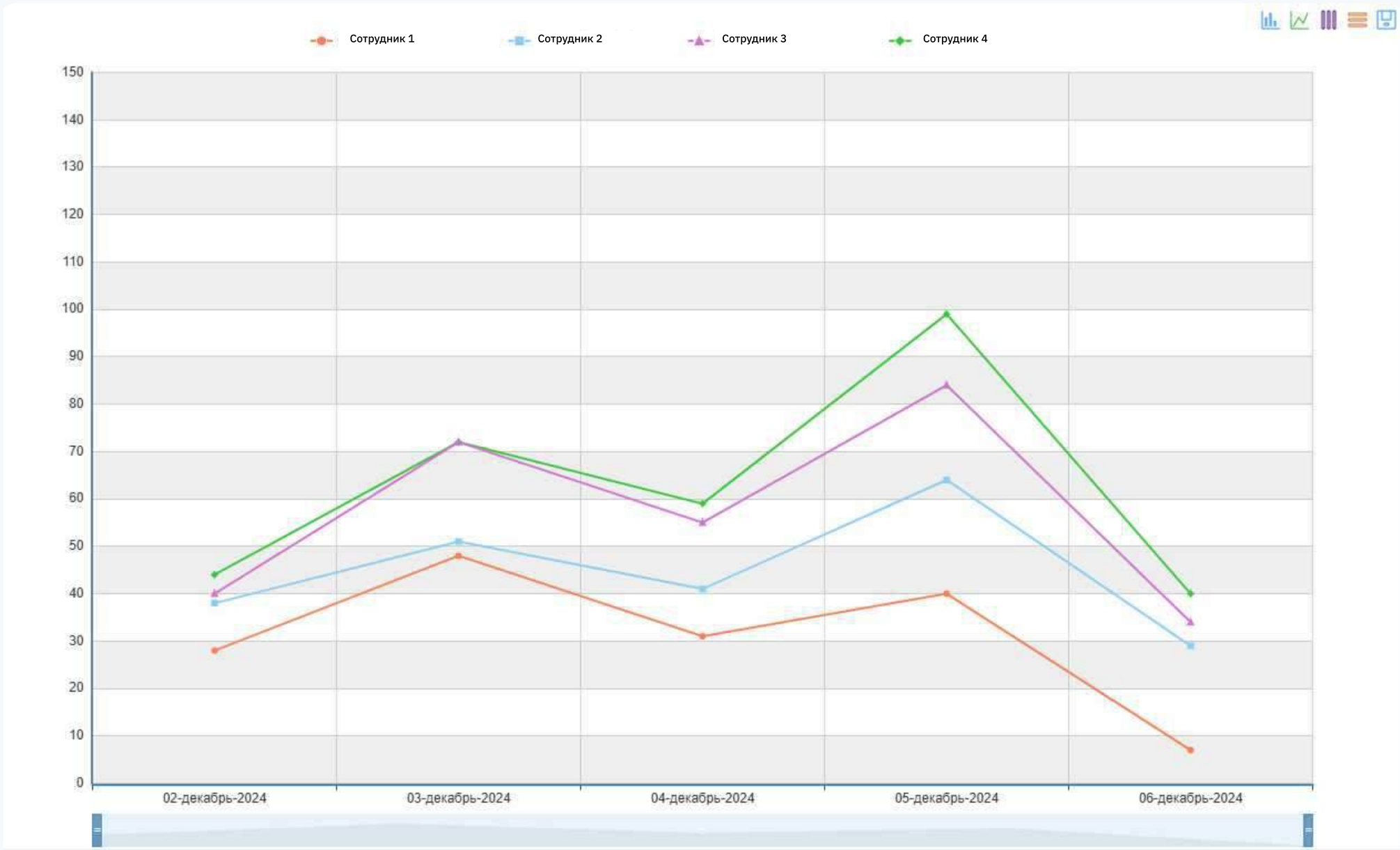


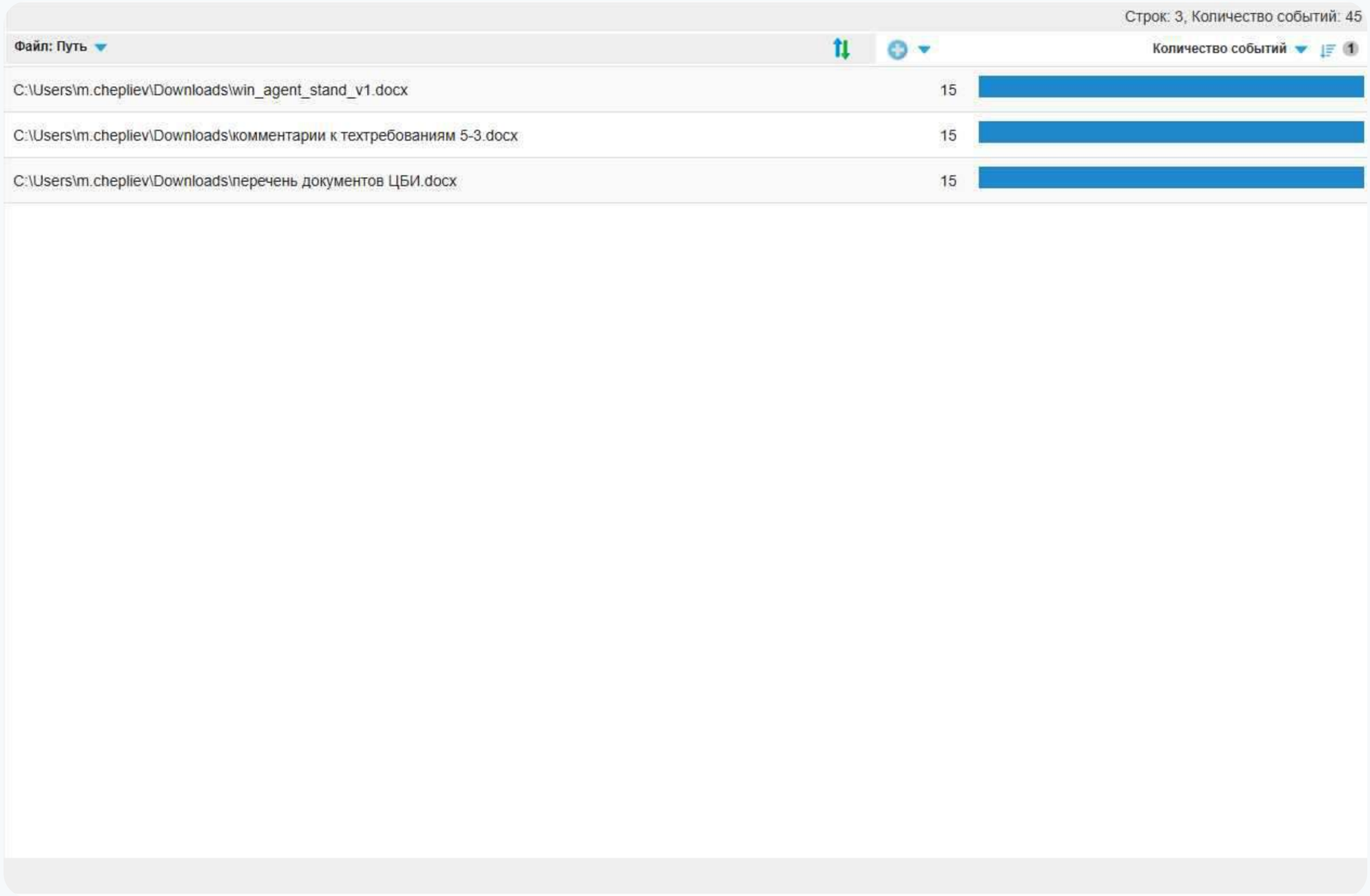
График взаимосвязей и анализ аномалий

Различные формы визуального анализа позволяют сформировать и наглядно отобразить переписку сотрудников, перемещение файлов, аномалии в рамках активности пользователя.



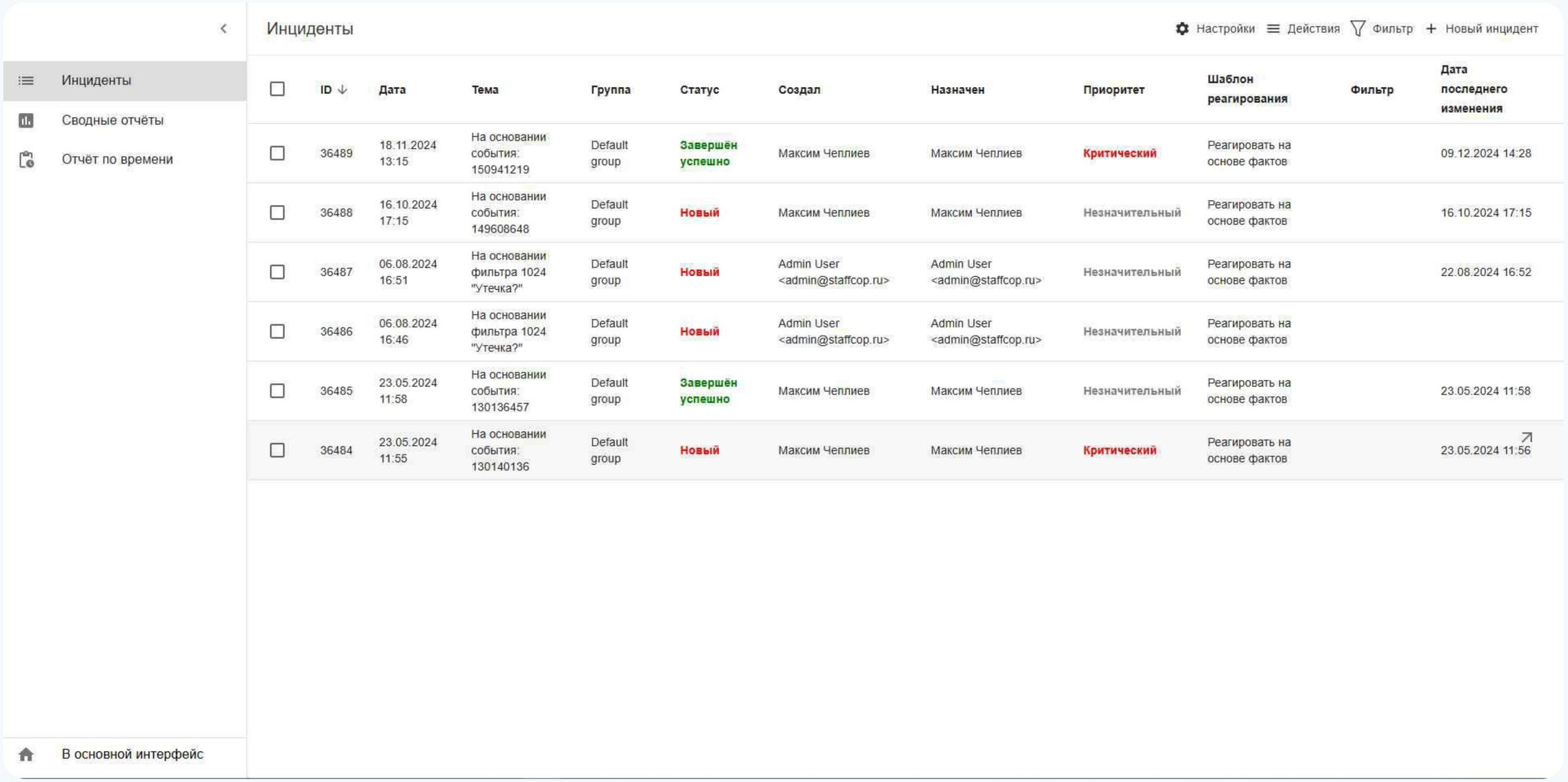
Метки для файлов

Не всегда можно выделить слова-триггеры в документах с конфиденциальной информацией. Установка в структуре самого файла метки, невидимой рядовому пользователю, позволяет не только контролировать движение файла в организации, но и ограничивать его перемещение и даже доступ пользователей к нему.



Консоль инцидентов

Помогает управлять задачами по расследованию инцидентов ИБ, что повышает эффективность работы. Консоль сокращает затраты за счёт управления процессом расследования и быстрого получения данных.

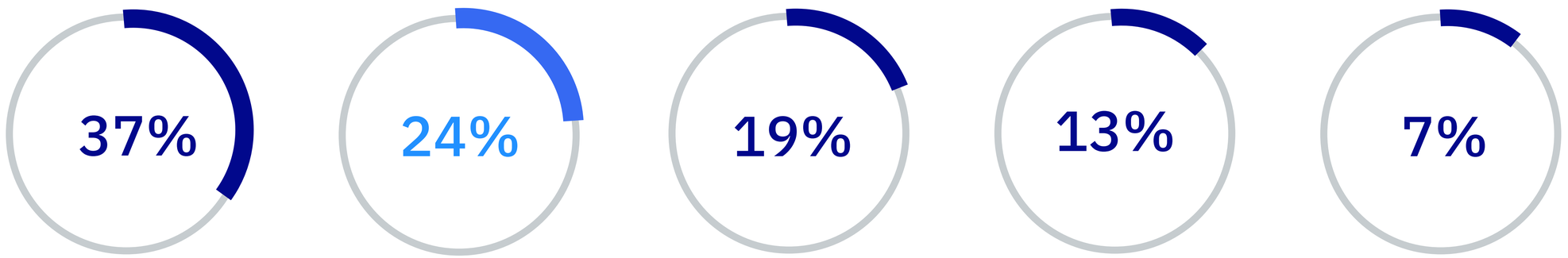


Учёт рабочего времени

Повышение эффективности труда

Мы опросили* наших клиентов, использующих Staffcop Enterprise, и составили картину распределения рабочего времени среднестатистического сотрудника.

Staffcop Enterprise не только фиксирует начало, перерывы и окончание рабочего дня, но и показывает детальную картину активности сотрудников.



* собственное исследование 000 «АТОМ БЕЗОПАСНОСТЬ», 2023 год

Гибкая настройка расписаний и категоризации приложений и сайтов

Для разных категорий сотрудников можно настроить список разрешённых программ и сайтов, а доступ к нежелательным ресурсам запретить. Кроме этого, настройки позволяют создавать уникальное расписание рабочего дня.

Название: Тестовое

Тип периода учета: Только рабочее расписани

Рабочие дни

День недели	Выбран	Начало работы	Окончание работы	Начало перерыва	Окончание перерыва	Рабочее время
Единое	☑	11:00	20:00	12:00	13:00	08:00
Понедельник	☑	11:00	20:00	12:00	13:00	08:00
Вторник	☑	11:00	20:00	12:00	13:00	08:00
Среда	☑	11:00	20:00	12:00	13:00	08:00
Четверг	☑	11:00	20:00	12:00	13:00	08:00
Пятница	☑	11:00	20:00	12:00	13:00	08:00
Суббота	☐					
Воскресенье	☐					

Наглядная статистика в отчётах и таблицах

— Опоздания
— Простои на работе
— Активное время за компьютером
— Продуктивное время
— Время, затраченное на личные нужды
— Статистика по сотрудникам и отделам

Staffcop Enterprise умеет в автоматическом режиме по расписанию отправлять подробный отчёт в PDF, HTML или XLS на электронную почту.

Топ активных	Кол-во
khalitov-win10x64	7ч 03м 31с
khalitov-win11x64	3ч 05м 26с
NICKSURWIN10x64	2ч 41м 16с
VERASURWIN10x64	21м 17с
sts-xps-u16	07м 10с
Achebykin-Win10-Pro	05м 10с
beta55	04м 00с
akleshchev-w64	03м 57с
astra-18	01м 50с

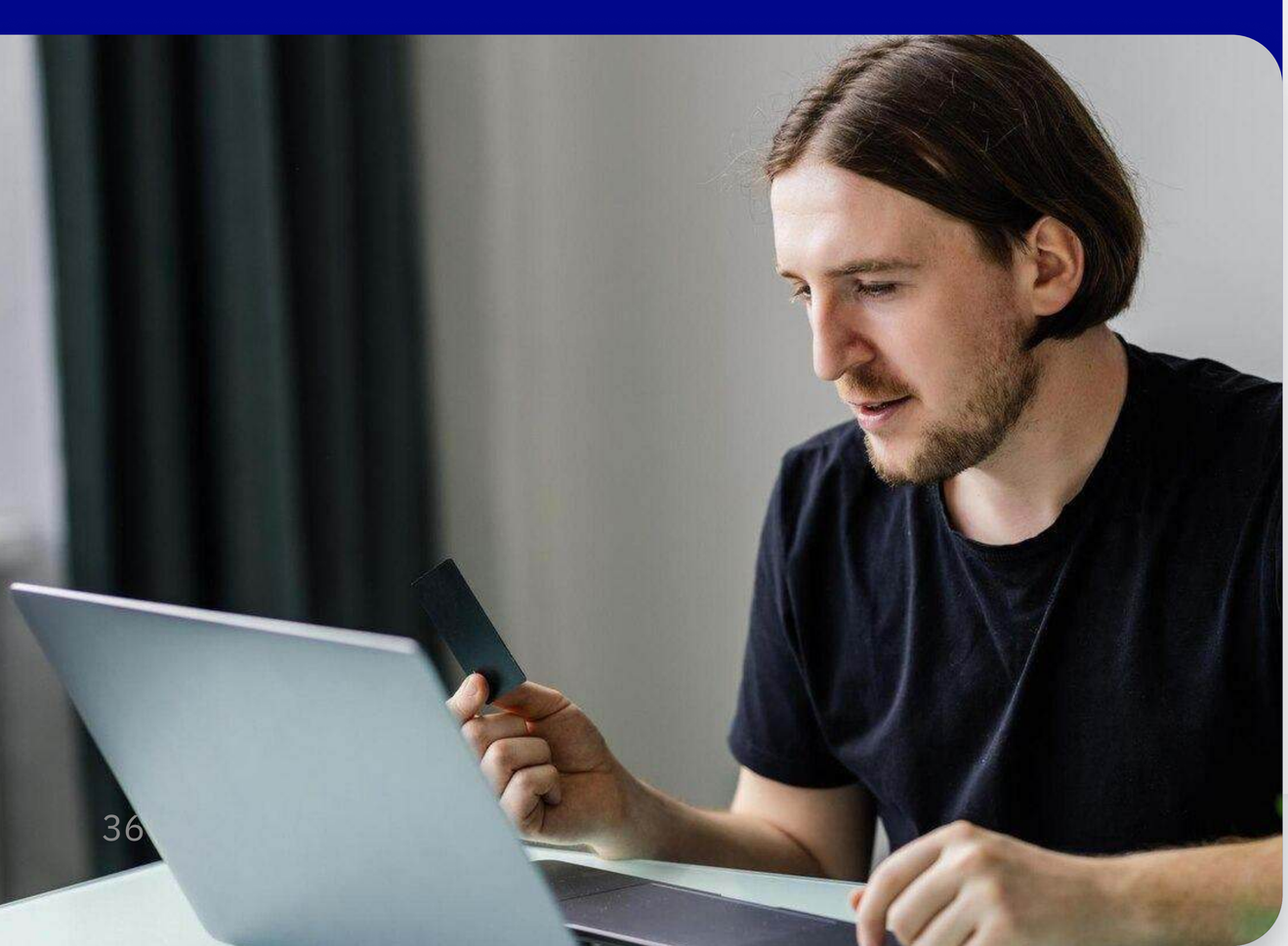
Топ неактивных	Кол-во
khalitov-win10x64	67ч 29м 10с
khalitov-win11x64	11ч 16м 35с
NICKSURWIN10x64	6ч 35м 49с
VERASURWIN10x64	1ч 01м 38с
beta55	17м 59с
sts-xps-u16	08м 58с
akleshchev-w64	02м 40с
Achebykin-Win10-Pro	02м 02с
astra-18	34с

Топ продуктивных	Кол-во
khalitov-win10x64	2ч 52м 19с
khalitov-win11x64	28м 29с
NICKSURWIN10x64	14м 41с
sts-xps-u16	06м 30с
Achebykin-Win10-Pro	05м 09с
VERASURWIN10x64	01м 24с
akleshchev-w64	22с

Топ непродуктивных	Кол-во
khalitov-win10x64	48с
astra-18	00с
akleshchev-w64	00с
Achebykin-Win10-Pro	00с
beta55	00с
VERASURWIN10x64	00с
NICKSURWIN10x64	00с

Блокировки

Staffcop Enterprise позволяет предотвратить утечку данных путём блокировки каналов передачи в формате чёрных или белых списков на компьютерах и терминальных серверах, умеет автоматически изменять уровень контроля за сотрудником при обнаружении подозрительных действий. Блокируйте файловые операции на основе правил.



- Блокировки запуска процессов и приложений
- Блокировка доступа к сайтам
- Блокировка по задаваемым группам файлов и идентификаторам
- Ограничение записи на съёмные носители
- Блокировка буфера обмена при передаче контента в другое приложение
- Блокировка операций с файлами по контенту, атрибутам и цифровым меткам
- Блокировка подключения к Wi-Fi сетям
- Блокировка носителей информации при превышении порога передачи данных
- Блокировка АРМ по команде сервера

Администрирование

Удалённое наблюдение за АРМ и перехват управления

Система предоставляет инструментарий для помощи администраторам.

В реальном времени можно не только удалённо подключиться к рабочей станции пользователя, чтобы проанализировать проблемы или детально изучить аномальную активность, но и получить доступ к управлению станцией. Например, чтобы оказать пользователю помощь или убрать из доступа нелегитимный файл.

Интеграция с SIEM, AD, 1С, СКУД и другими системами ИБ и ИТ

Staffcop Enterprise позволяет работать с другими информационными системами, чтобы передавать или дополнять данные. Например, информация о присутствии сотрудников на работе поступает от СКУД или 1С. При расследования инцидентов данные из других систем могут передаваться в SIEM с помощью Syslog или API.

Администрирование

Изменение конфигурации контроля при наступлении события

Не всегда у администратора есть возможность оперативно среагировать на инцидент.
При аномалиях в активности пользователя система автоматически изменяет набор правил для работы агента. Таким образом пользователь будет переведён под особый, более плотный контроль.

Ролевой доступ

Система решает широкий спектр задач и зачастую для этого не нужен доступ ко всем её элементам.
В системе используется широкий набор прав для администраторов, позволяющий ограничить доступ вплоть до просмотра нужного отчёта.
Также можно предоставить доступ для управления системой, но ограничить доступ к данным.

Тестируйте уже сейчас!

Быстро

Развёртывание пилотного проекта обычно занимает не более одного дня

Легко

Требуется минимум усилий и ресурсов для запуска

Комплексно

Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение

Бесплатный аудит

Позволит вскрыть точки роста в вашей системе ИБ

Staffcop Enterprise — единственное решение для мониторинга и защиты данных, сочетающее выгодную стоимость владения и лучший уровень клиентского сервиса без компромиссов в функциональности.

Контур
staffcop

Расследование инцидентов
внутренней безопасности

Техническая поддержка

+7 499 638-71-52
support@staffcop.ru

Отдел продаж

+7 499 653-71-52
sales@staffcop.ru

Приёмная

+7 495 129-04-92

Россия, г. Новосибирск,
ул. Кутателадзе 4Г, 3-й этаж

ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop.ru