



DLP система StaffCop

Программный комплекс для контроля информации,
действий пользователей и системных событий
на рабочих компьютерах

Программный комплекс для контроля информации,
действий пользователей и системных событий на рабочих
компьютерах

Безопасность, эффективность и администрирование в одном продукте



Расследование инцидентов

StaffCop — это машина времени! В любой момент можно вернуться назад и посмотреть, что делал тот или иной сотрудник в указанном промежутке времени.

Обнаружение утечек информации

Система имеет гибкую настройку фильтров и оповещений, поэтому возможную утечку или вторжение удаётся обнаружить на ранней стадии, чем существенно сократить последствия.



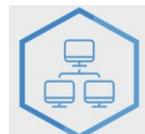
Анализ поведения пользователей

Автоматический анализ появления аномалий. Удобные средства статистической визуализации: тепловые диаграммы, граф и дерево взаимосвязей.



Мониторинг бизнес-процессов

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



Удаленное администрирование

С уведомлением или без уведомления пользователя. Удалённый захват управления ПК. Удобно работать IT-специалистам и службе ИБ.



Инвентаризация компьютеров

Полная картина использования программных продуктов и аппаратного обеспечения. Интенсивность использования и архив состояний.



Учет рабочего времени

Мониторинг активности пользователя за ПК. Учет фактически отработанного времени, опозданий, ранних уходов, прогулов и простоев.



Оценка продуктивности сотрудников

Разделение использование программ, посещения сайтов на продуктивные и непродуктивные. Настройка для отдельных пользователей, групп и отделов. Сравнение показателей.

ТОТАЛЬНЫЙ КОНТРОЛЬ



Передача гипертекстовой информации

и файлов:

— HTTP / HTTPS

— FTP / FTPs

USB-порты

— контроль и блокировка

Теневое копирование файлов

— из электронной почты

— со съемных носителей

— переданных через интернет

— отправленных на печать

Почтовые протоколы:

— SMTP / SMTPs

— IMAP

— POP3 / POP3s

— MS Exchange

Декодирование сервисов веб-почты и

социальных сетей:

— mail.ru, yandex.ru, gmail.com...

— VK, FB, Одноклассники, LinkedIn...

Интернет-мессенджеры

— Skype

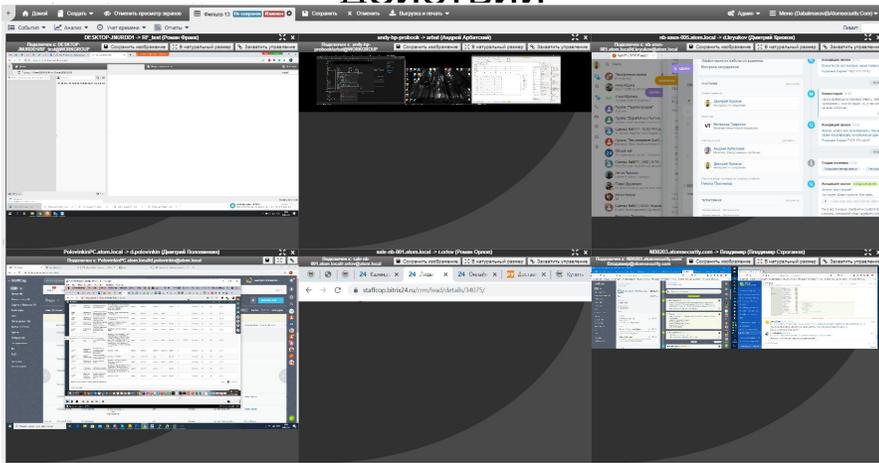
— ICQ, QIP, Jabber (XMPP)

— Mail.ru Agent

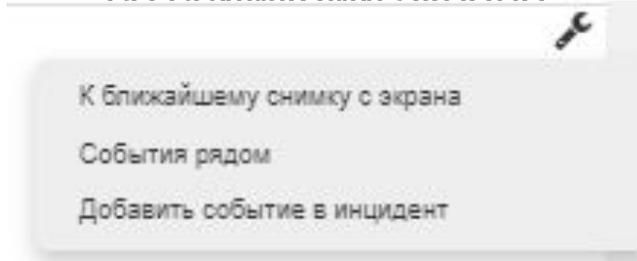
— Yahoo и другие

ЗАПИСЬ СЕССИЙ ПОЛЬЗОВАТЕЛЕЙ

Квадратор – перехват управления ПК и фиксация действий



Корреляция действий
пользователя
со снимками экрана

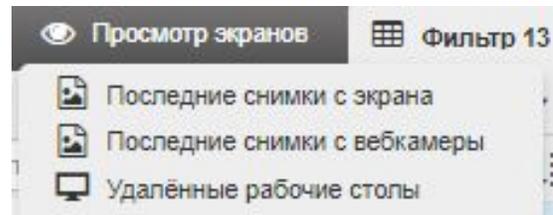


Запись
звука

Запись звука

<input type="checkbox"/>	Запись с микрофона	Вести запись с обнаруженных микрофонов. Требует вклю
<input type="checkbox"/>	Запись звука колонок	Вести запись звука колонок. Требует включения модуля. ¶
Длительность отрывков, секунда:	<input type="text" value="600"/>	Вести запись отрывками указанной длительности.
Уровень записи, от 0 до 100:	<input type="text" value="80"/>	Уровень записи в процентах от 0 до 100. Для использован
Интервал тишины:	<input type="text" value="5"/>	Интервал тишины в секундах, после которого запись зву
Качество записи:	<input type="text" value="0"/>	Качество записи: Диапазон [-2147483648;2147483647] • <0 - FM Radio Stereo, 28.8 Kbps> • =0 - CD quality, 64 Kbps • >0 - Better than CD quality, 128 Kbps Stereo
Шумовой порог, от -100 до 100:	<input type="text" value="0.0"/>	Игнорировать звуки при уровне сигнала ниже заданного.

Запись с веб-
камер



РАССЛЕДОВАНИЕ ИНЦИДЕНТОВ ИБ

Конструктор многомерных отчетов

С помощью последовательного наложения фильтров и применения операторов «и» «или» «не» позволяет «на лету» получить необходимый набор данных с агрегированной информацией по количеству событий. Конструктор поддерживает 30 событий и 64 измерения. Технология Drill down.

Сквозной поиск по словам и регулярным выражениям

Выявление ключевым словам и регулярным выражениям до минимума сократит время расследования инцидента

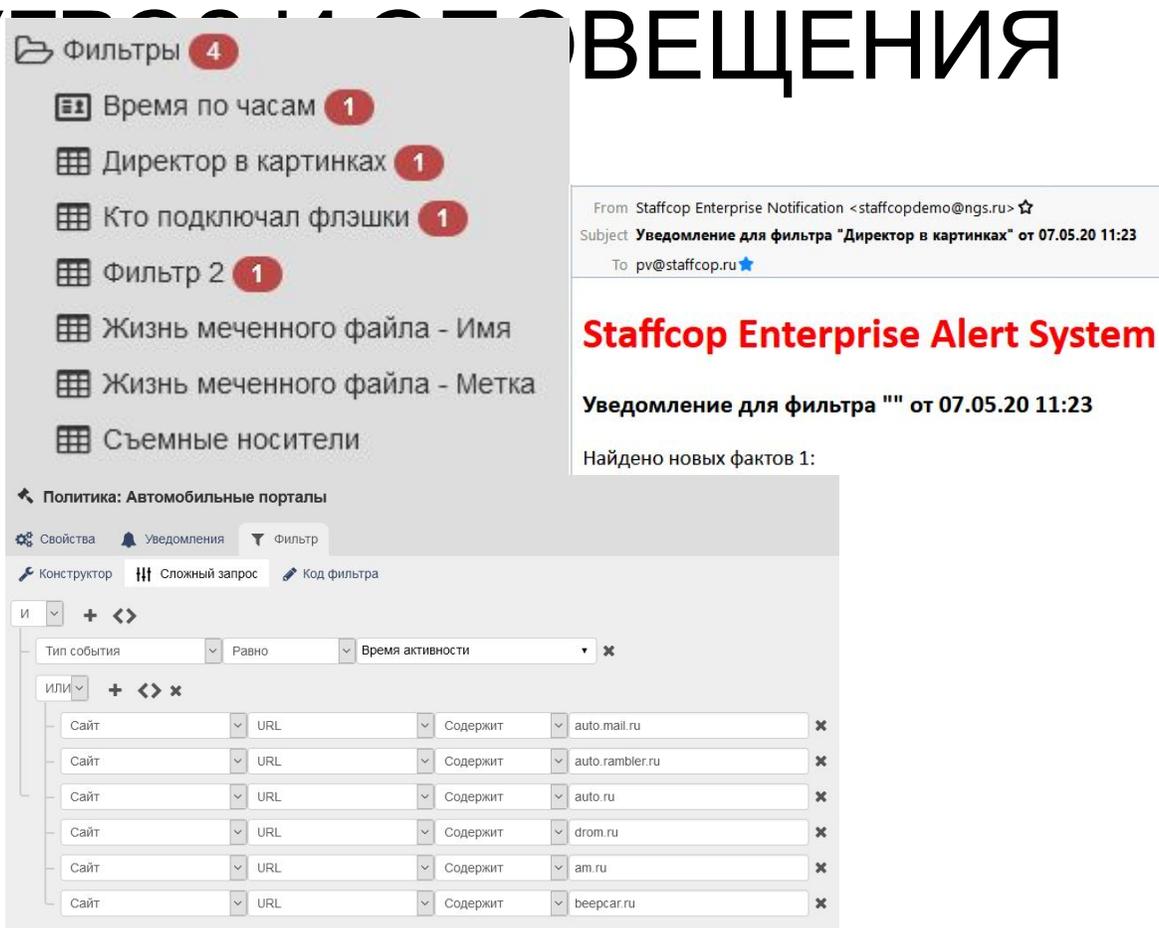
Множество графов и диаграмм (инфографика)

для выявления аномального поведения, анализа изменений интенсивности событий. Линейные, круговые и тепловые диаграммы, графы взаимосвязей.



СОВРЕМЕННЫЕ ИНСТРУМЕНТЫ ОБНАРУЖЕНИЯ

УВЕДОМЛЕНИЯ И ОПОВЕЩЕНИЯ



The screenshot displays the Staffcop Enterprise Alert System interface. On the left, a sidebar shows a list of filters with red notification counts: "Время по часам" (1), "Директор в картинках" (1), "Кто подключал флэшки" (1), "Фильтр 2" (1), "Жизнь меченного файла - Имя", "Жизнь меченного файла - Метка", and "Съемные носители". Below the filters, the "Политика: Автомобильные порталы" is selected. The main area shows a notification email from "Staffcop Enterprise Notification <staffcopdemo@ngs.ru>". The subject is "Уведомление для фильтра 'Директор в картинках' от 07.05.20 11:23" and the recipient is "pv@staffcop.ru". The email content includes the title "Staffcop Enterprise Alert System" and the message "Уведомление для фильтра '' от 07.05.20 11:23". Below the email, it states "Найдено новых фактов 1:". At the bottom, the "Конструктор" (Builder) is visible, showing a filter rule: "Тип события" (Type of event) is "Равно" (Equal) and "Время активности" (Activity time) is "Время активности". The rule is composed of several conditions connected by "ИЛИ" (OR): "Сайт" (Site) "URL" "Содержит" (Contains) "auto.mail.ru", "Сайт" "URL" "Содержит" "auto.rambler.ru", "Сайт" "URL" "Содержит" "auto.ru", "Сайт" "URL" "Содержит" "drom.ru", "Сайт" "URL" "Содержит" "am.ru", and "Сайт" "URL" "Содержит" "beercar.ru".

- **Событийный анализ данных**
Анализ данных на предмет инцидентов по выпадающим событиям из общего списка
- **Контентный анализ файлов**
Парсинг файлов на наличие в них конфиденциальной или потенциально опасной информации, в том числе графических форматов
- **Система оповещений**
Уведомления о нарушениях появляются как в панели администрирования, так и могут быть немедленно отправлены по электронной почте
- **Поиск подобных документов**

АНАЛИЗ ПОВЕДЕНИЯ ПОЛЬЗОВАТЕЛЕЙ

Определение количественных отклонений от шаблонной модели поведения пользователей на основе собранного массива данных.

Поиск по словарям позволяет определить приоритетные темы и эмоциональную составляющую

Агрегированная карточка пользователя



ИНВЕНТАРИЗАЦИЯ И ПАСПОРТИЗАЦИЯ

Изъятие оперативной памяти

Инвентаризация - Устройства				
Статус ↓	Компьютер ↓	Производитель ↓	Тип устройства ↓	HWID ↓
❗ Отсутствует	DESKTOP-SL7A47M		RAM: Physical Memory 0 Bytes: 8589934592	<input type="text"/>
❗ Отсутствует	DESKTOP-SL7A47M	Microsoft	Network Adapter: RAS Async Adapter	SW\{EEAB7790-C514-11D1-B42
❗ Отсутствует	DESKTOP-SL7A47M	(Standard system devices)	Mouse: USB Input Device	USB\VID_046D&PID_C07716&24
✅ В наличии	DESKTOP-SL7A47M	(Standard disk drives)	Disk Drive: ST9500325AS	SCSI\DISK&VEN_&PROD_ST95
✅ В наличии	DESKTOP-SL7A47M	Alps Electric	Mouse: Alps Pointing-device	ACPI\AUI201314&1B6B5F90&0

Установка некорпоративного ПО

✅ В наличии	NB0001.atomsecurity.com	UmyyVideoDownloader		1.10.3.2
✅ В наличии	NB0001.atomsecurity.com	Kasparov Chessmate		
✅ В наличии	DESKTOP-SL7A47M	MSI to EXE Setup Converter 2.3.0.6		
✅ В наличии	DESKTOP-SL7A47M	Windows Setup Remediations (x64) (KB4023057)		
✅ В наличии	DESKTOP-SL7A47M	Shrew Soft VPN Client		
✅ В наличии	PC0051.atomsecurity.com	WIX Toolset v3.11.1.2318	.NET Foundation	3.11.1.2318
✅ В наличии	DESKTOP-SL7A47M	1С:Предприятие 8 (учебная версия) (8.3.8.1933)	1C	8.3.8.1933

АДМИНИСТРИРОВАНИЕ

Мониторинг и управление

- удаленный рабочий стол
- сетевой трафик
- процессы и приложения
- установка и удаление ПО



Блокировка

и

- приложений и сайтов
- съемных USB-устройств по черному и белому списку

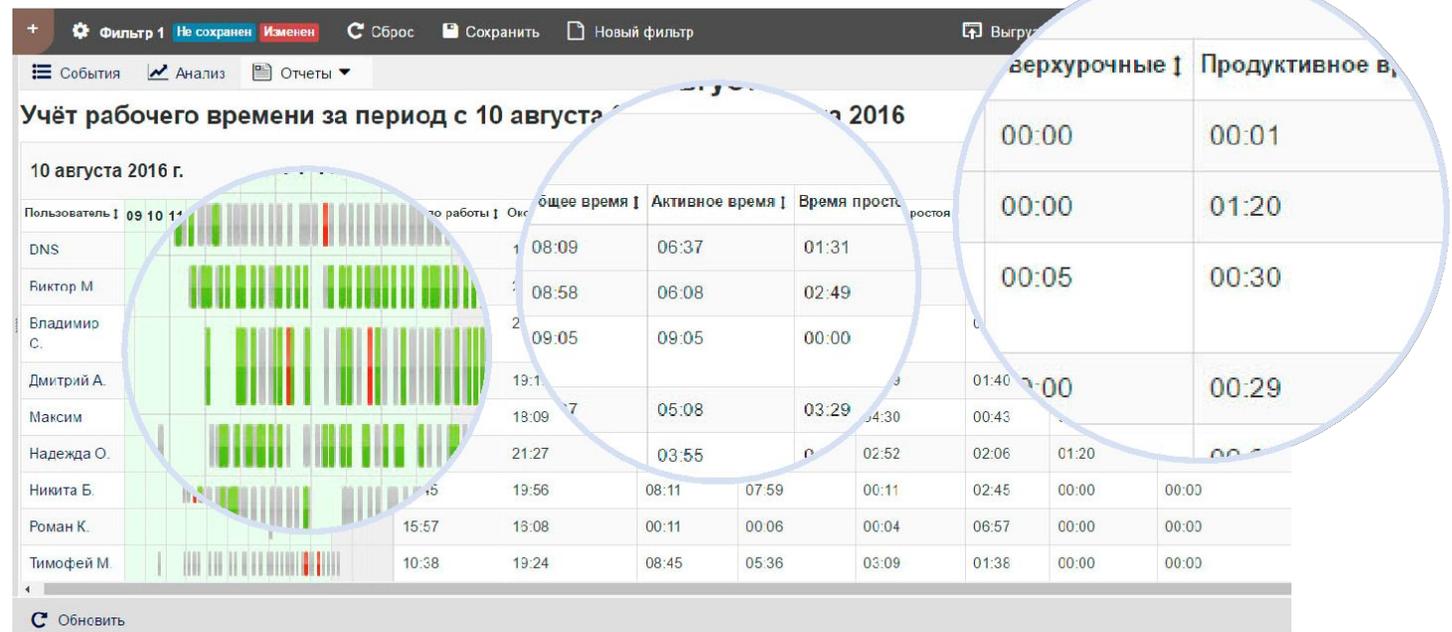
Принудительное отключение

- предупреждение и выключение по расписанию
- блокировка действий пользователя в режиме реального времени

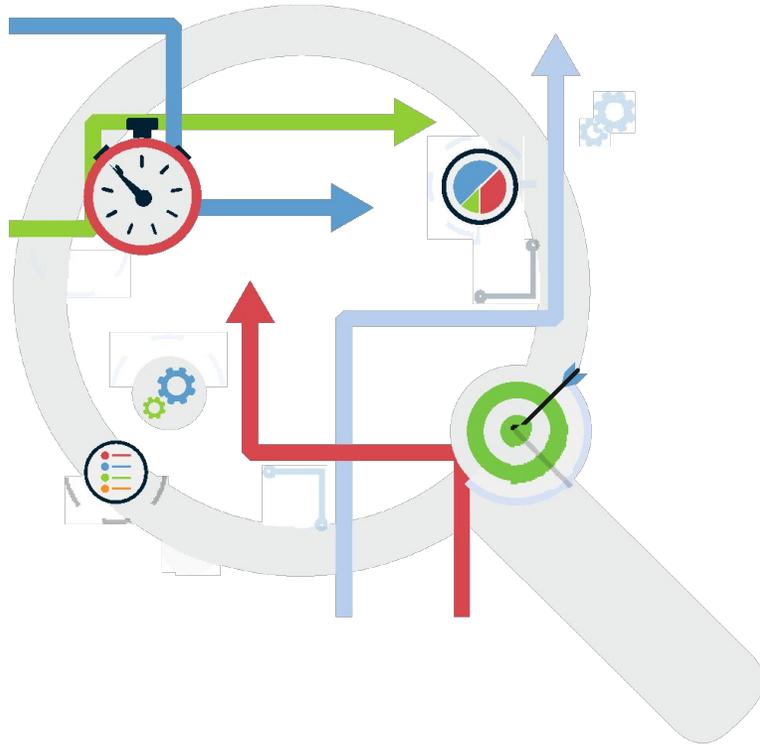


УЧЁТ РАБОЧЕГО ВРЕМЕНИ И ОЦЕНКА ЕГО ЭФФЕКТИВНОСТИ

- Продуктивная деятельность
- Непродуктивная деятельность
- Нейтральная деятельность
- Не было активности



ОПТИМИЗАЦИЯ БИЗНЕС-ПРОЦЕССОВ



Со StaffCop легко контролировать бизнес-процессы, находить «узкие» места и выявлять блокирующие факторы, а также расследовать причины их появления.

Отслеживать реальный KPI сотрудников, например, для менеджеров продаж - это может быть количество отправленных коммерческих предложений и договоров, количество контактов с клиентами и поставщиками.



ИНТЕГРАЦИЯ СО СТОРОННИМИ СИСТЕМАМИ

- Коннектор для загрузки данных в систему из сторонних источников
возможность интеграции данных из сторонней системы: СКУД, IP-телефония, календарь Outlook, MS Exchange
с отрисовкой данных в отчётах и графиках, создание кастомизированных отчётов на основе собранных данных
- Коннектор для SIEM - расширенный syslog с возможностью получения запросов таблицы фактов по ТЗ заказчика, и дальнейшей передачи лога в SIEM-систему для настройки политик
- Коннектор для выгрузки данных в сторонние системы BI
возможность выгрузки данных в стороннюю системы с отрисовкой данных в отчётах, графиках и иных видах отображения информации
- Разработка дополнительных инструкций пользователя и администратора под ГОСТ и требования регуляторов
- Создание Backup, распределение хранения данных для обеспечение отказоустойчивости системы.
- Доработка функционала под заказчика и т.д.
- Адаптеры под ОС семейства Linux

ПРИОРИТЕТНАЯ ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

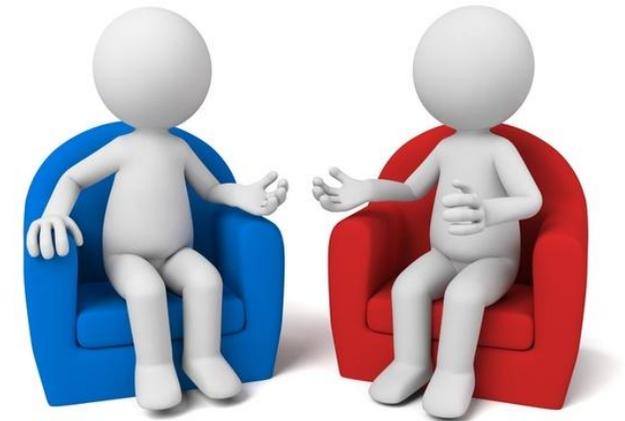
Обращениям присваивается статус наивысшего приоритета, время реакции уменьшается по почте до **30** минут, по телефону – в режиме **реального времени** выделенному



- Первичная поддержка
- Аварийно-восстановительная поддержка
- Профилактическая поддержка
- Экспертная тех. поддержка включает в себя
- Четыре плановых выезда инженера на площадку заказчика по Москве и Московской области

Удобные каналы коммуникации,

- общий чат с инженером 2-го уровня,
- прямой телефон, e-mail
- удаленное подключение.



ПРЕИМУЩЕСТВА



Многомерные аналитические отчеты и схемы коммуникаций и движения информации с возможностью перехода от общего к частному.



Мониторинг и управление рабочими местами из единого веб-интерфейса, возможность просто и безопасно организовать доступ из любой точки интернета.



Работа в любых сетевых инфраструктурах — подойдет для контроля распределенной филиальной сети, удаленных офисов и сотрудников.



Уникальные функции мониторинга рабочих станций и терминалов серверов под управлением GNU/Linux систем — расширяет возможности контроля.



Построено на решениях с открытым исходным кодом — не требуется приобретать дополнительные лицензии на серверную ОС и базы данных.



Быстрая работа на больших объемах данных за счет использования современных баз данных ClickHouse и PostgreSQL на технологии OLAP-кубов.



Подробная документация, оперативная и компетентная техническая поддержка. Команда проекта обеспечивает полноценное сопровождение с начального этапа тестирования.



Возможность доработки под требования, интеграции с другими системами и бизнес-процессами заказчика.



Минимальные требования к «железу», разумная стоимость и бессрочные лицензии, как результат — низкая стоимость приобретения, внедрения и эксплуатации



СЕРТИФИКАТ ФСТЭК

Программный Комплекс StaffCop Enterprise соответствует «Требованиям к средствам контроля съемных машинных носителей информации, ФСТЭК России», утвержденных Приказом ФСТЭК России от 28 июля 2014 г. N 87 - по 4 классу защиты и «Профиль защиты средств контроля подключения съемных машинных носителей информации четвертого класса защиты (ИТ. СКН.П4.ПЗ)» (ФСТЭК России, 2014), заданию по безопасности АЛМЮ.501410.СКЭ4-01.ЗБ и оценочному уровню доверия ОУДЗ (усиленный) в соответствии ГОСТ Р ИСО/МЭК 15408.

Сертификат ФСТЭК4 №4234 от 15.04.2020



Спасибо за внимание



Выполнил студент ОГБПОУ «РКЭ» группы
ИБ-416:
Чуланов Арсений Алексеевич

Принял:
Преподаватель:
Власова Светлана Владимировна