



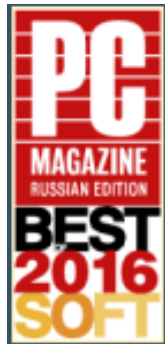
Контроль над информационными потоками и действиями сотрудников на удаленке и в офисе.

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность
m.chepliev@staffcop.ru





- Более 10 лет разработки приложений контроля сотрудников;
- Академгородок, Новосибирск, резиденты Технопарка и Сколково;
- Высокотехнологичная компания, ~50 сотрудников.
- Наша цель: «доступные решения задач информационной безопасности»
- Продано ~1300 серверных компонентов, ~ 66 000 АРМ за 2019-й год.
- Продано ~2200 серверных компонентов, ~ 171 000 АРМ за 2020-й год.



Технопарк Новосибирского Академгородка



ФСТЭК России
Федеральная служба
по техническому и
экспортному контролю



Минкомсвязь
России





Комплексное решение по информационной безопасности, учёту рабочего времени и контролю эффективности сотрудников



Своевременное обнаружение и предотвращение угроз ИБ и ЭБ
Организованное расследование инцидентов
Анализ деятельности сотрудников



Учет рабочего времени и оценка продуктивности сотрудников
Мониторинг бизнес-процессов и анализ эффективности сотрудников



Инвентаризация программного и аппаратного обеспечения
Удаленное администрирование машин пользователей

Сложности контроля удаленного доступа

Контроль рабочих процессов

- Продуктивность ненормированного рабочего дня
- Эффективность выполнения задач
- Аудит

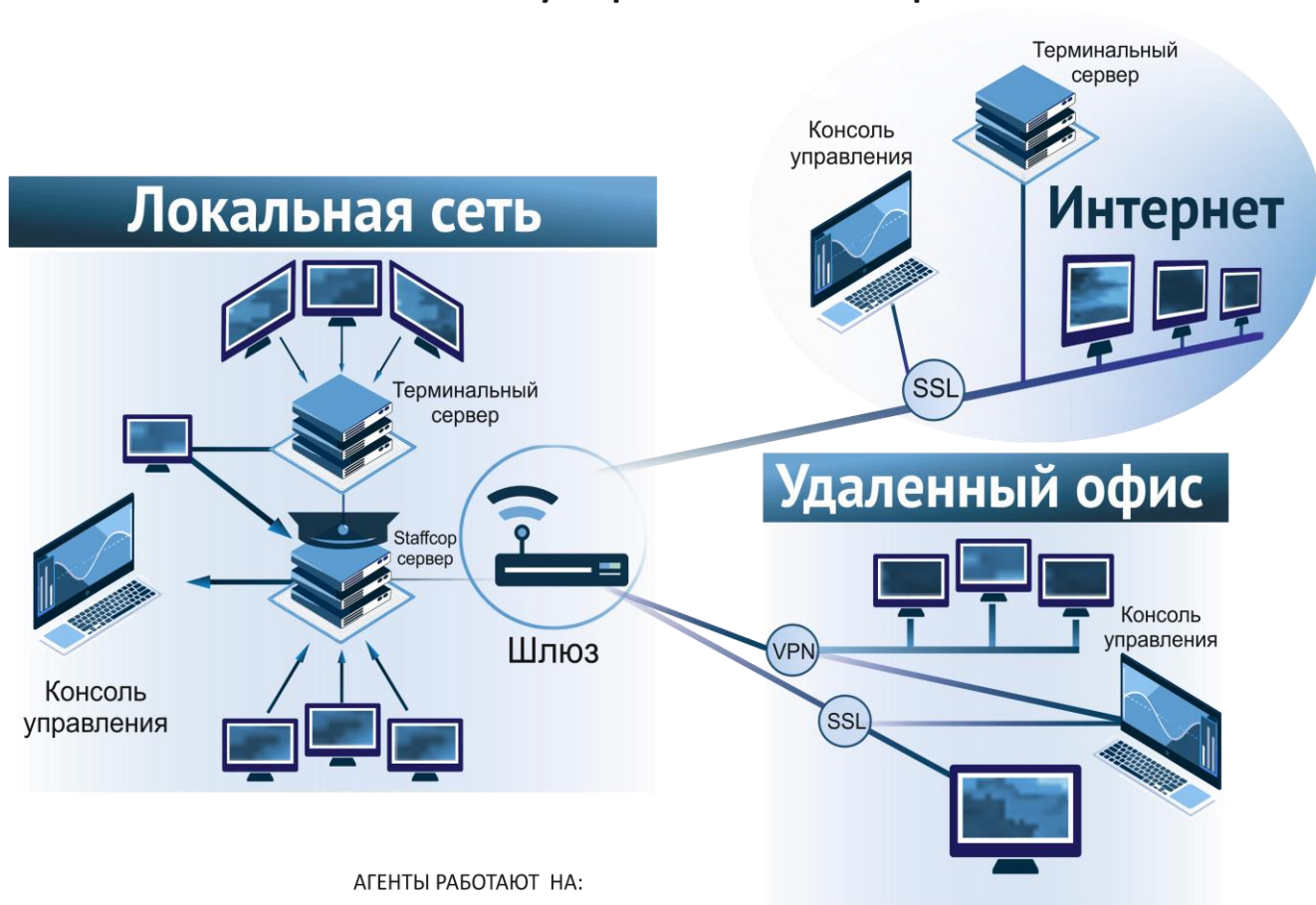
Контроль доступа к информации

- Обеспечение контроля взаимодействия
- Доступ к информации
- Передача информации

Аутентификация

- Контроль надежности доступа.
- Контроль доступа к учетной записи

Как устроен Staffcop:



АГЕНТЫ РАБОТАЮТ НА:



Сервер использует базу данных Postgresql и работает на операционной системе ubuntu



Контроль ПК под управлением различных OS:

Windows, Linux, MacOS

Множество способов установки агентов, как локальные, так и удаленные.

Для организации сервера достаточно одной виртуальной машины и система готова к сбору сразу после установки

Инвентаризация «железа» и ПО

Снимки с веб-камер

Мониторинг посещенных сайтов и поисковых запросов

Мониторинг действий в социальных сетях

Контроль email-переписки

Контроль USB и CD

Мониторинг доступа к файлам



Сканирование хранящихся файлов

Скриншоты и запись видео рабочего стола

Подключение к рабочему столу

Контроль печати

Перехват сообщений в мессенджерах

Кейлоггер

Запись аудио с микрофона и колонок

Копия файла на сервере

- Электронная почта
- Съёмные носители
- Передача через интернет
- Печать на принтере

USB-порты

- Контроль подключений
- Операции с файлами
- Блокировка накопителей
- Черные и белые списки

Интернет-мессенджер

- Skype
- ICQ, QIP, Jabber(XMPP)
- Mail.ru, Yahoo
- Telegram

Передача гипертекстовой информации и файлов

- HTTP/HTTPS
- FTP/FTPS
- POST и GET запросы

Почтовые протоколы

- SMTP/SMTSPS
- IMAP
- POP3/POP3S
- MAPI (MS Exchange)

Декодирование сервисов веб-почты и соц.сетей

- Mail.ru, Yandex.ru, gmail.com и т.п.
- VK, FB, Одноклассники и т.п.

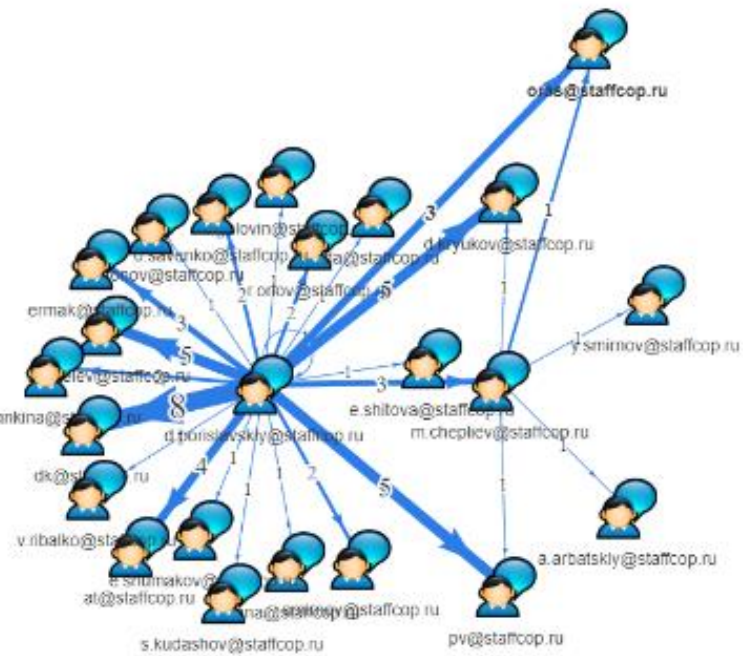
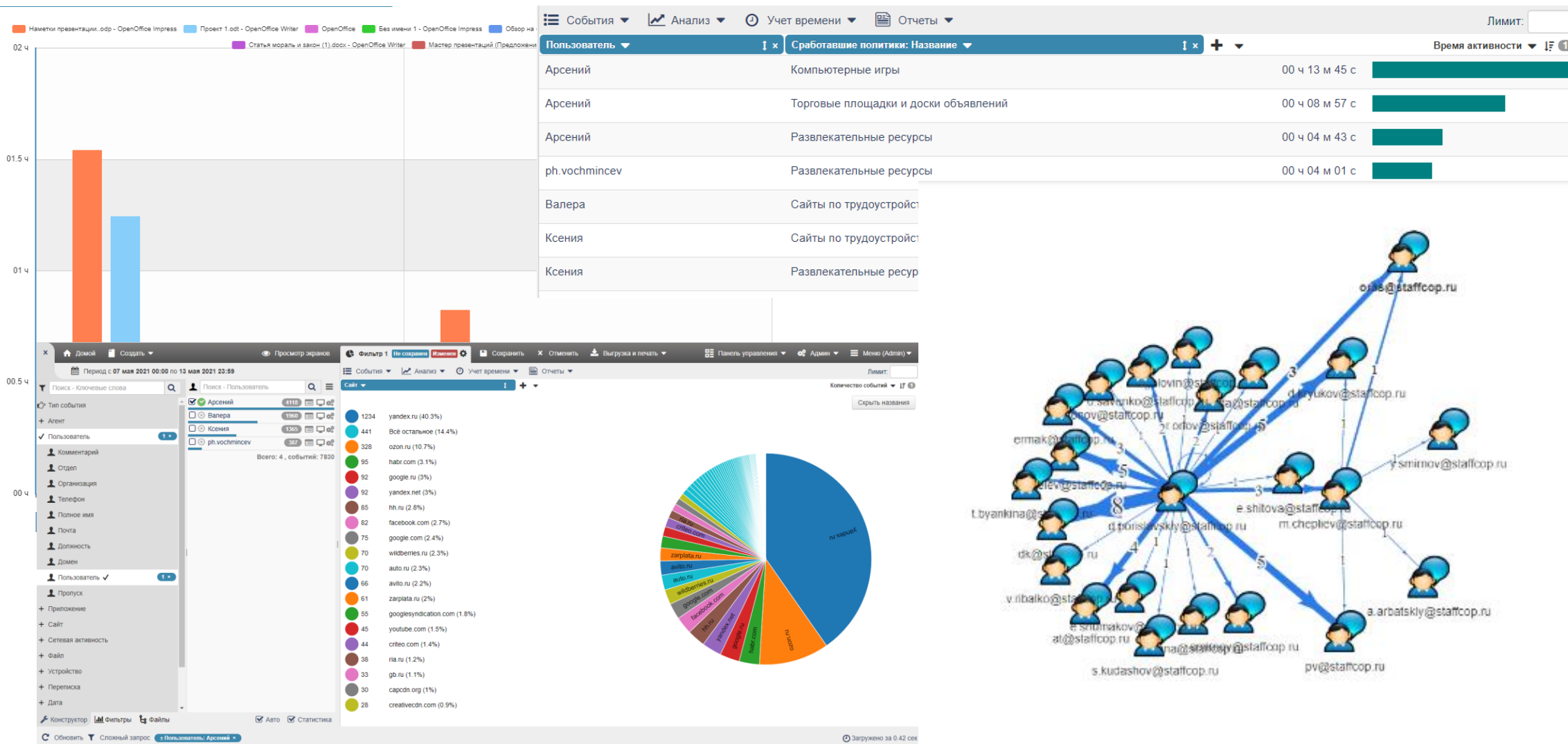
Контроль рабочих процессов осуществляющихся посредством удаленного доступа



- Долгосрочный архив событий
- Конструктор многомерных отчетов
- Создание словарей и поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений по инцидентам
- Гибкая система фильтрации информации



Анализ собранной информации



Организация расследований ИНЦИДЕНТОВ

В основной интерфейс Инциденты Фильтр + Новый инцидент

Инциденты	ID ↓	Дата	Тема	Группа	Статус	Создал	Назначен	Приоритет	Шаблон реагирования	Фильтр
Статусы	13	01.06.2021 13:17	На основании фильтра 1010 "Поиск по словарю 3"	Утечка данных		Admin User	Maxim Chepliev	Незначительный	Найти утечку	Конфиденциальная информация
Группы инцидентов	12	01.06.2021 13:07	На основании фильтра 1010 "Поиск по словарю 3"	Утечка данных		Admin User	Maxim Chepliev	Незначительный	Найти утечку	Конфиденциальная информация
Шаблоны реагирования	11	26.05.2021	На основании фильтра	Утечка данных		Admin User	Maxim	Незначительный	Ограничить доступ к данным и каналам	Фильтр 1
Сводные отчеты										

Недоменная отправка файлов

Переписка: Отправитель ↓

kkasperova522@gmail.com	5	тра	Утечка данных	Admin User
arseniieset@ngs.ru	4	тра	Наличие недопозволенной информации	Admin User

Отправка на флешку

Пользователь: Полное имя ↓ Устройство: ID устройства ↓

Нет данных за период, попадающих под фильтр

Фильтр 1

- 39 Конфиденциальная информация (18.7%)
- 27 Пароль в браузере (12.9%)
- 20 Развлекательные ресурсы (9.6%)
- 18 Торговые площадки и доски объявлений (8.6%)

Поиск по словарю: Конфиденциальная информация

⚙ Свойства 🔔 Уведомления ⚙ Фильтр

Активировать уведомления

Регулярность: Новые
 Ежедневно
 Еженедельно
 Ежемесячно 1 числа

Время отправки:

Создать инцидент

Шаблон реагирования:

Группа инцидента:

Кому:



Словари, фильтры и политики

Поиск по словарю: Конфиденциальная информация

Свойства | Уведомления | Фильтр

Активировать уведомления

Регулярность: Новые, Ежедневно, Еженедельно, Ежемесячно числа

Время отправки:

Создать инцидент

Шаблон реагирования:

Группа инцидента:

Сложный запрос | Код фильтра

ИЛИ | + Условие | Группа условий

- ИЛИ | + Условие | Группа условий
 - Тип события | Равно | Перехваченный файл
 - Тип события | Равно | Файл
- ИЛИ | + Условие | Группа условий
 - Пользователь | Пользователь | Не равно | Ксения
 - Пользователь | Пользователь | Не равно | Арсений
- ИЛИ | + Условие | Группа условий
 - Текст | Содержит | Договор

Поиск по словарю: Кредитные карты

Свойства | Уведомления | Фильтр

Название:

Категория:

Политика активна

Продолжить выполнение

Применить к новым событиям

Применить ко всем событиям

Внимание! Включение политик

Подсветка найденного:

Словарь:

```
~(((4\d{3}))((5[1-5]\d{2}))((6011))((34\d{1}))((Z0-9|_|+\.)+)?>\s*)*\d{4}\s*(?:<[a-zA-Z0-9]#WHERE array_length(find_credit_cards
```

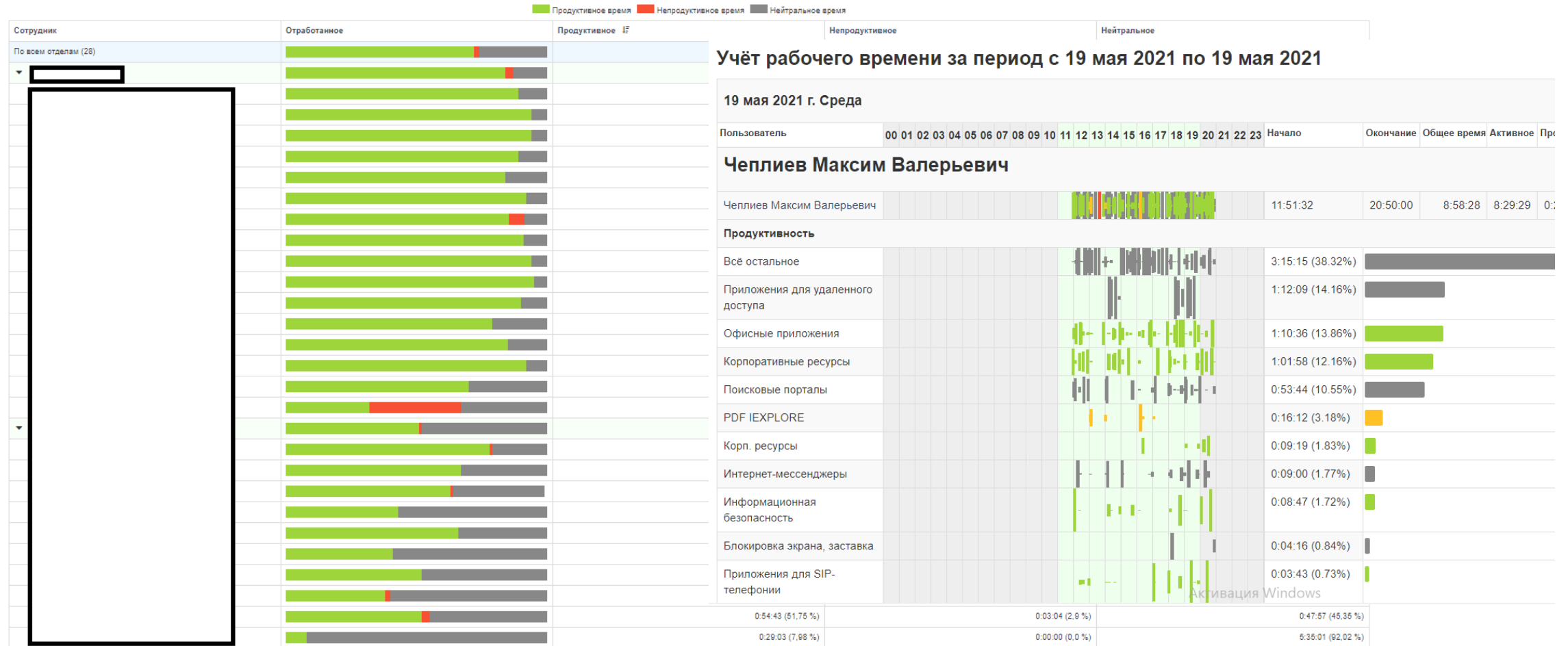
Политики

- Политики продуктивности
- Политики безопасности
- Словарь ненормативной лексики
- Словарь наркоманского сленга
- Словарь откатной тематики
- Словарь поиска работы
- Кредитные карты
- Словарь алкогольной тематики
- Словарь подарки
- Словарь долги
- Словарь религиозной тематики
- Паспорт
- ИНН
- СНИЛС
- Перехват Print Screen
- Поиск Staffcop
- Шифрованный архив
- Пароль в браузере

Учет рабочего времени

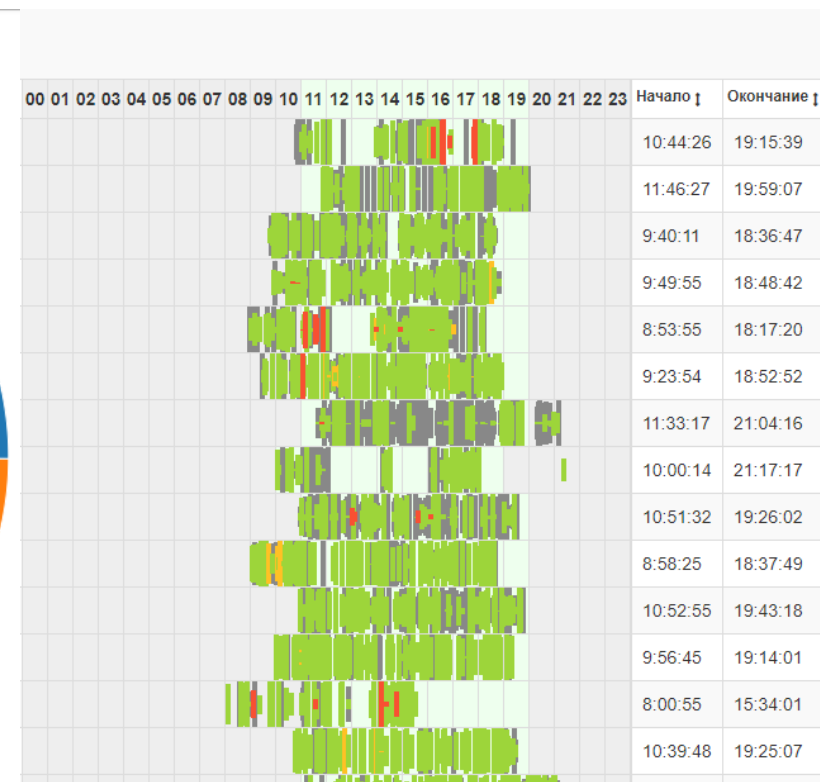
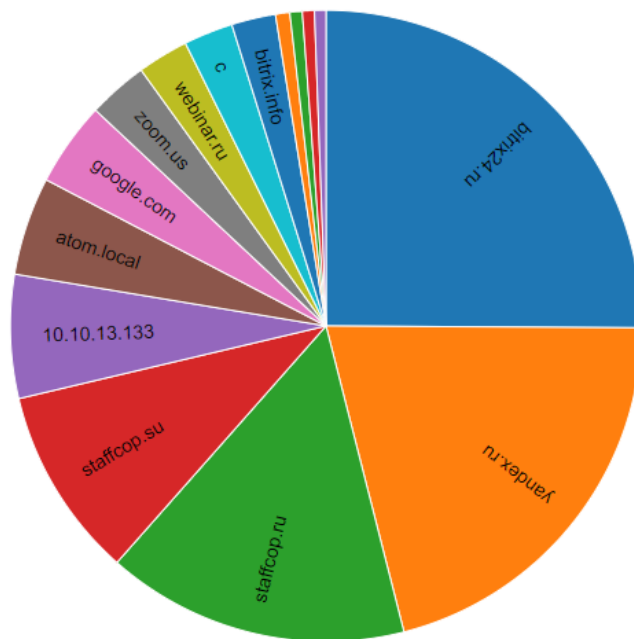
Продуктивное время за период с 31 мая 2021 по 31 мая 2021

Отчёт отражает суммарное продуктивное/непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя



Анализ эффективности

- 12244 bitrix24.ru (25.1%)
- 10214 yandex.ru (20.9%)
- 7561 staffcop.ru (15.5%)
- 4772 staffcop.su (9.8%)
- 3088 10.10.13.133 (6.3%)
- 2455 atom.local (5%)
- 2105 google.com (4.3%)
- 1495 zoom.us (3.1%)
- 1275 webinar.ru (2.6%)
- 1232 c (2.5%)
- 1102 bitrix.info (2.3%)
- 357 10.10.13.98 (0.7%)
- 309 crocotime.com (0.6%)
- 300 servermall.ru (0.6%)
- 285 yandex.net (0.6%)



Staffcop 2021 диджитал - PowerPoint

00:24:34



Staffcop код ИБ - PowerPoint

00:02:26



Staffcop_май_хабаровск - PowerPoint

00:01:39



Staffcop_январь - PowerPoint

00:01:19



Мониторинг

Блокировки

Инвентаризация ПО и «железа»

Уровни доступа к данным и функционалу в системе

Интеграция с SIEM

Метки и блокировка доступа

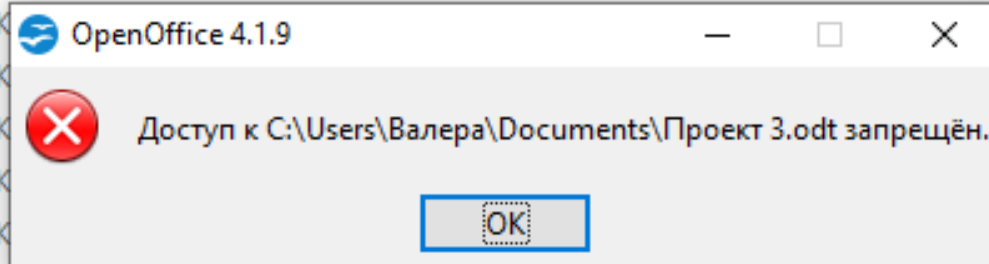
Справка

DLP модуль **Внимание!** Включение модуля активирует анализ контента файлов, что может привести к замедлению работы компьютера

Конфигурация DLP модуля: [Правила блокировки контента](#), см. [документацию](#). Скачать утилиту для пометки файлов для [Windows](#) или [Linux](#)

Поле	Оператор	Значение	Добавить выражение
1 правило:			
Имя пользователя	equals	Ксения	Удалить правило 
And			
Контент	matches	<input type="text" value=""/>	And 
And			
Имя приложения	equals	outlook.exe	<input type="text" value=""/> 

Презентация Оре...	17 КБ
Adobe Acrobat D...	186 КБ
Текстовый докум...	24 КБ
Текстовый докум...	9 КБ
Презентация Оре...	14 КБ
Текстовый докум...	9 КБ
Текстовый докум...	9 КБ
Текстовый докум...	9 КБ



Блокировка каналов утечки

Правила: Блокировка - Приложения

Блокировать - блокировать запуск приложений по имени. Не внесённые в список приложения не блокируются.
Разрешить - список разрешенных приложений по имени.

Блокировать	+
teamviewer.exe	x

Правила: Блокировка - Сайты 16 / 0

Блокировать - блокировка сайтов по адресу домена.
Разрешить - список сайтов разрешенных для посещения, указывается в виде доменного имени.

Сайт	Домен	URL	
Блокировать			+
web-api/upload-attachment			x
userstorage.mega.co.nz/ul/			x

- USB устройства Контроль подключений и отключений USB-устройств. Перехват файловой активности и создание теневых копий файлов, скопированных на USB-накопители. Требует включения модулей "Файлы > Файловая активность и Теневое копирование".
- Блокировать USB накопители Блокировка всех USB-накопителей. Перекрывает правила мониторинга "Блокировка USB" и "Блокировка - USB-класс". Требует включение модуля "USB устройства"
- USB накопители только для чтения Переводит все USB-накопители в режим "Только чтение". Требует включение модуля "USB устройства"
- Блокировать CD накопители Блокировка CD-накопителей.

Правила: Блокировка - USB

Блокировать - блокировка всех «Device ID» указанных в списке.
Разрешить - блокировка всех «Device ID» за исключением тех, что указаны в данном списке.

Блокировать	+
-------------	---

Разрешить	+
USB\VID_090C&PID_1000\0113000000000602	x

Фильтр: *цен* в перехваченных файлах

Свойства | Уведомления | Фильтр

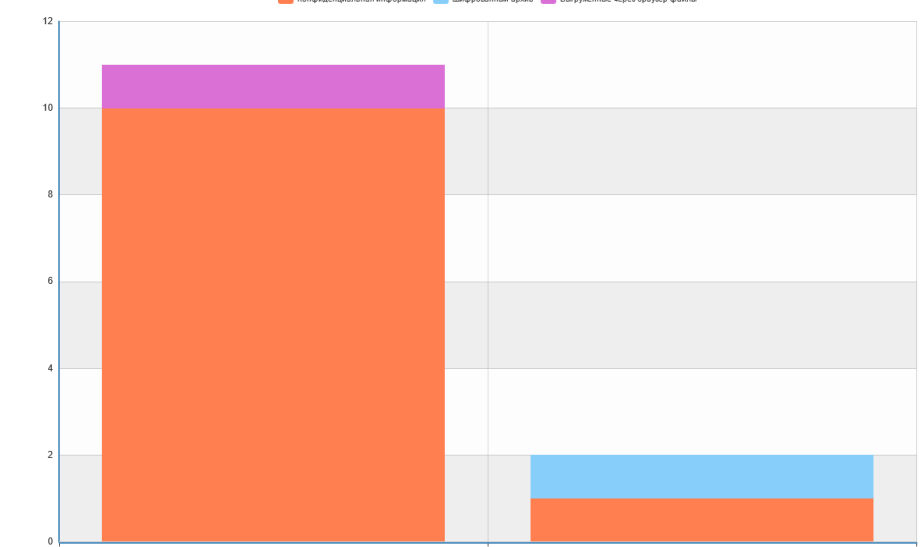
Конструктор | Сложный запрос | Код фильтра

И | + Условие | Группа условий

Файл | Имя файла | Содержит | цен

Пользователь | Сработавшие политики: Название

Количество событий



Период с 01 января 2021 00:00 по 31 декабря 2021 23:59

- С:
 - Users
 - Арсений
 - Desktop
 - Рабочая
 - 1000 сотрудников.docx
 - 10000 сотрудников.docx
 - 1500 сотрудников.docx
 - 2000 сотрудников.docx
 - 2500 сотрудников.docx
 - 3000 сотрудников.docx
 - 4000 сотрудников.docx
 - 5000 сотрудников.docx
 - 6000 сотрудников.docx
 - 7000 сотрудников.docx
 - 8000 сотрудников.docx
 - 9000 сотрудников.docx
 - требования-с-ETL до 10K.xlsx
 - Методички
 - Методичка по УРВ.pdf
 - Сервер.docx
 - УРВ на удалёнке (автореферат).pdf
 - Аналитика
 - Валера

Фильтр 5 | Не сохранен | Изменен | Сохранить

События | Анализ | Учет времени

Время	Тип	Компьютер	Поль
2021-06-01 13:17:25	Файл	Arsenii	
2021-05-14 14:34:29	Файл	Arsenii	

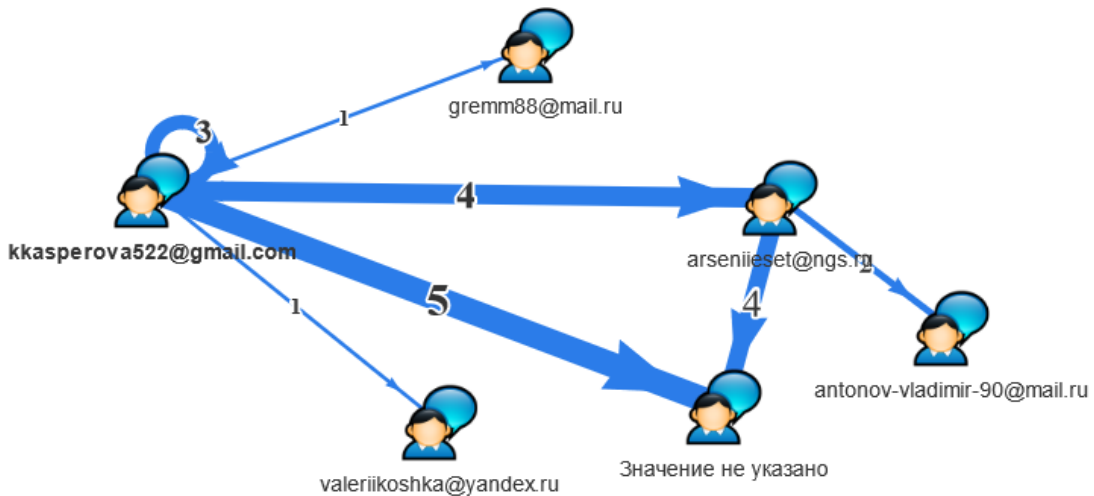
Время 2021-06-01 13:17:25

Содержимое Учёт рабочего времени для сотрудников на «удалёнке» с использованием программного комплекса StaffCop Enterprise

Недоменная переписка, мессенджеры и передача информации конкурентам.

Пользователь ▾	↑ x	Переписка: Канал общения ▾	↑ x	Переписка: Отправитель ▾	↑ x	+	▾	Количество событий ▾	1
Ксения		Telegram		Maxim_Chepliev_79232470277				14	

Время ↓	Компьютер	Пользователь	Приложение	Получатели	Контент	Размер	Связано с
2021-05-17 14:00:56	DESKTOP-N36I35U	Ксения	chrome.exe	Ксения	Скачать Цены.docx ↓	2.2 Kb	Mail →
2021-05-17 13:38:44	DESKTOP-N36I35U	Ксения	outlook.exe	Арсений	Скачать RE: Проверка связи.html ↓	6 Kb	Mail →
2021-05-17 10:30:38	Arsenii	Арсений	thunderbird.exe	Ксения	Скачать Проверка связи.html ↓	5.2 Kb	Mail →
				Maxim_Chepliev_79232470277	Скачать Проверка связи.html ↓	4.2 Kb	Mail →
				kkasperova522@gmail.com	Скачать Проверка связи.html ↓	184 B	Mail →
				arseniieset@ngs.ru	Скачать Проверка связи.html ↓	1.6 Kb	Mail →
				-90@mail.ru	Скачать Fwd: сохранить.html ↓	1.4 Kb	Mail →
					Скачать Re: Проверка связи.html ↓	17.2 Kb	Mail →
					Скачать Шаблон трудового договора.zip ↓	1.7 Kb	Mail →
					Скачать staffc.html ↓		



Нерегламентированное ПО и извлечение оборудования.

+ Security Update for Microsoft Office 2016 (KB3114690) 32-Bit Edition

Microsoft Edge		
Статус	Компьютер	Поставщик
Добавлено	DESKTOP-N36I35U	Корпорация Майкрософт
В наличии	Arsenii	Корпорация Майкрософт
Отсутствует	DESKTOP-N36I35U	Корпорация Майкрософт

+ Update for Microsoft Office 2016 (KB4011631) 32-Bit Edition

+ Update for Microsoft OneNote 2016 (KB4011137) 32-Bit Edition

+ Security Update for Microsoft Office 2016 (KB4011185) 32-Bit Edition

+ Security Update for Microsoft Word 2016 (KB4011643) 32-Bit Edition

+ Update for Microsoft Office 2016 (KB3115281) 32-Bit Edition

+ Update for Microsoft Office 2016 (KB4011225) 32-Bit Edition

TeamViewer

Статус	Компьютер	Поставщик
В наличии	DESKTOP-N36I35U	TeamViewer

+ Update for Microsoft OneDrive for Business (KB3141458) 32-Bit Edition

+ Update for Microsoft Office 2016 (KB2920684) 32-Bit Edition

Фильтр 19 Сохранить Отменить Выгрузка и печать

Панель управления Админ Меню (Ph.vochmincev@atom.local)

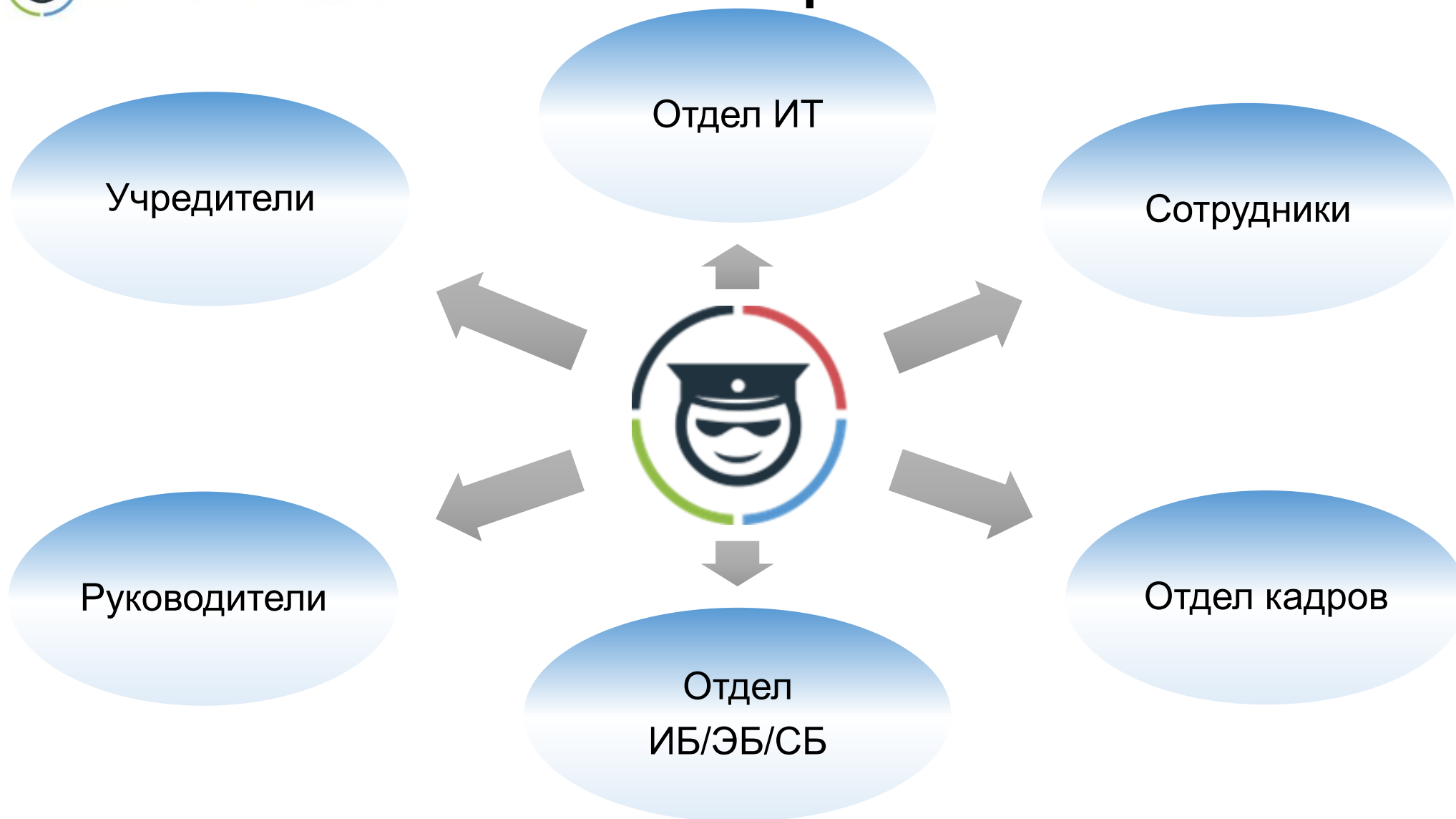
События Анализ Учет времени Отчеты Лимит:

Инвентаризация - Устройства

Статус	Компьютер	Производитель	Тип устройства	HWID	Дата наличия
Отсутствует	support-07	Logitech	INPUT: Logitech USB Optical Mouse 2Mbit/s	/0/100/12/1/3	16:15:39 06.07.2021
Отсутствует	support-07	Manufacturer0	MEMORY: 4.0G DIMM Synchronous 1600 MHz (0.6 ns) #SerNum0	/0/2d/0	16:15:39 06.07.2021
Отсутствует	support-07		MEMORY: 8.0G System Memory	/0/2d	16:15:39 06.07.2021
Отсутствует	support-07	Manufacturer1	MEMORY: 4.0G DIMM Synchronous 1600 MHz (0.6 ns) #SerNum1	/0/2d/1	16:15:39 06.07.2021
Отсутствует	support-07	Advanced Micro Devices, Inc. [AMD/ATI]	STORAGE: SB7x0/SB8x0/SB9x0 SATA Controller [IDE mode]	/0/100/11	16:15:39 06.07.2021
Отсутствует	support-07	Advanced Micro Devices, Inc. [AMD/ATI]	DISPLAY: RS780L [Radeon 3000] /dev/fb0	/0/100/1/5	16:15:39 06.07.2021
Отсутствует	support-07	Linux 5.8.0-59-generic ohci_hcd	BUS: OHCI PCI host controller @usb5 12Mbit/s	/0/100/13/1	16:15:39 06.07.2021
Отсутствует	support-07	System manufacturer	SYSTEM: System Product Name (To Be Filled By O.E.M.) #System Serial Number #03000200-0400-0500-0006-000700080009		16:15:39 06.07.2021
Отсутствует	support-07	Linux 5.8.0-59-generic ohci_hcd	BUS: OHCI PCI host controller @usb4 12Mbit/s	/0/100/12.1/1	16:15:39 06.07.2021
Отсутствует	support-07		INPUT: HDA ATI SB Line	/0/100/14.2/2	16:15:39 06.07.2021
Отсутствует	support-07		SYSTEM: Motherboard registers	/0/100/14.3/0	16:15:39 06.07.2021
Отсутствует	support-07	Linux 5.8.0-59-generic ohci_hcd	BUS: OHCI PCI host controller @usb6 12Mbit/s	/0/100/13.1/1	16:15:39 06.07.2021
Отсутствует	support-07	Advanced Micro Devices, Inc. [AMD/ATI]	STORAGE: SB7x0/SB8x0/SB9x0 IDE Controller @scsi1	/0/100/14.1	16:15:39 06.07.2021
Отсутствует	support-07	Advanced Micro Devices [AMD]	PROCESSOR: AMD Phenom(tm) II X2 555 Processor #To Be Filled By O.E.M.	/0/4	16:15:39 06.07.2021
Отсутствует	support-07	ASUSTeK Computer INC.	BUS: M4A78LT-M-LE #MB-1234567890	/0	16:15:39 06.07.2021

Диск заполнен на 67% Загружено за 66.87 сек

Кто заинтересован в этом?



Почему мы?



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



Мониторинг и анализ событий на рабочих местах из единого веб-интерфейса, возможность просто и безопасно организовать доступ к серверу



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



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



Возможность доработки под требования заказчика, в том числе, интеграции с другими системами и бизнес-процессам заказчика



Staffcop подходит для выполнения требований банковских ГОСТов, приказов ФСТЭК России и для работы на объектах КИИ

Количество компьютеров	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	3 350 Р / 1 ПК	1 117 Р / 1 ПК
26–50	3 050 Р / 1 ПК	1 017 Р / 1 ПК
51–150	2 990 Р / 1 ПК	997 Р / 1 ПК
151–250	2 890 Р / 1 ПК	963 Р / 1 ПК
251–500	2 790 Р / 1 ПК	930 Р / 1 ПК
501–1000	2 690 Р / 1 ПК	897 Р / 1 ПК
1000+	2 590 Р / 1 ПК	863 Р / 1 ПК

Бессрочная лицензия – по запросу



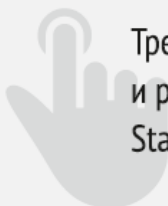
Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро



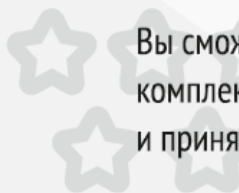
Развертывание пилотного проекта обычно занимает не более одного дня

Легко



Требуется минимум усилий и ресурсов для запуска StaffCop Enterprise

Комплексно





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



Благодарю за внимание!

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность

 +7(499)6382809 доб. 238
 m.chepliev@staffcop.ru