Система контроля для обеспечения комплекса мер защиты информационных и технологически процессов.

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

STAFFCOP

- 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.

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016

PC MAGAZINE RUSSIAN EDITION BEST 2016 SOFT

Sk Сколково

академпарк
Технопарк Новосибирского Академгородка

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

Минкомсвязь России

infosecurity RUSSIA

BIS SUMMIT 2018

STAFFCOP

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

Задачи и цели контроля.

Зачем?

- Надежность
- Сложность контроля

Как?

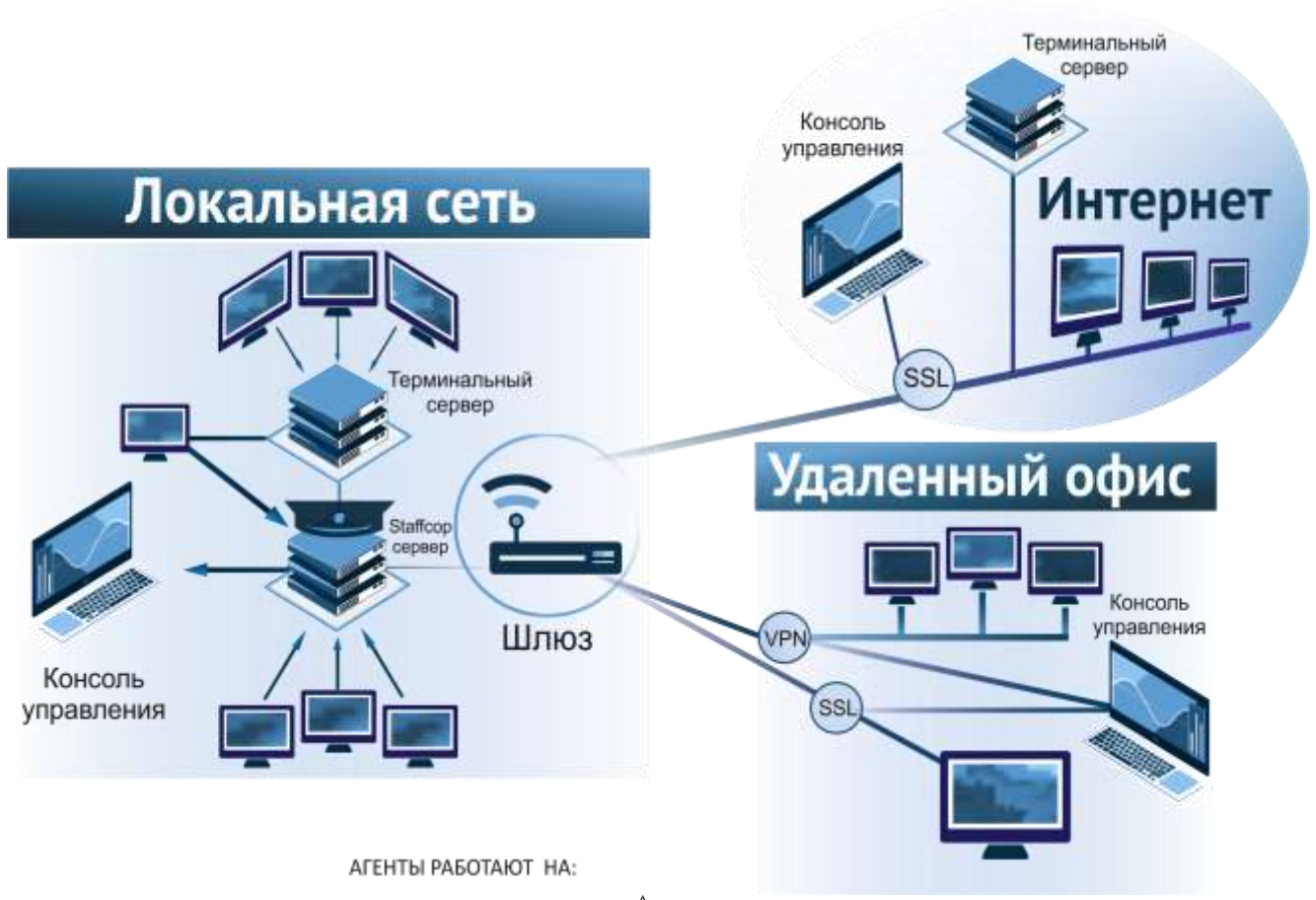
- Оперативность
- Точность
- «Невмешательство»

Что?

- Люди
- Процессы
- Технологии

Наше решение

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

Полный контроль за объектом защиты

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

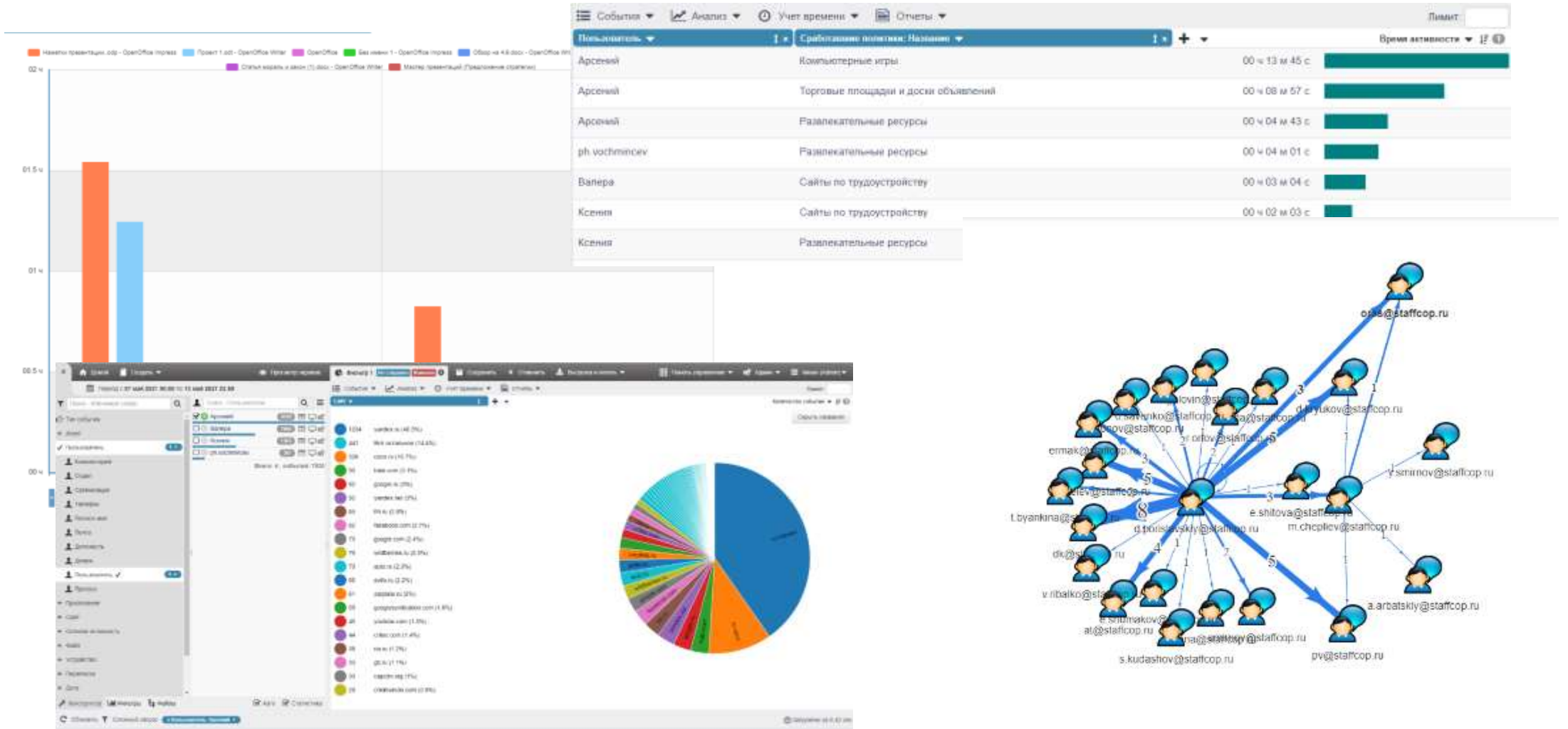
Запись аудио с микрофона и колонок

Копия файла на сервере	USB-порты	Интернет-мессенджер	Передача гипертекстовой информации и файлов	Почтовые протоколы	Декодирование сервисов веб-почты и соц.сетей
•Электронная почта •Съемные носители •Передача через интернет •Печать на принтере	•Контроль подключений •Операции с файлами •Блокировка накопителей •Черные и белые списки	•Skype •ICQ, QIP, Jabber(XMPP) •Mail.ru, Yahoo •Telegram	•HTTP/HTTPS •FTP/FTPS •POST и GET запросы	•SMTP/SMTPS •IMAP •POP3/POP3S •MAPI (MS Exchange)	•Mail.ru, Yandex.ru, gmail.com и.т.п. •VK, FB, Одноклассники и.т.п.

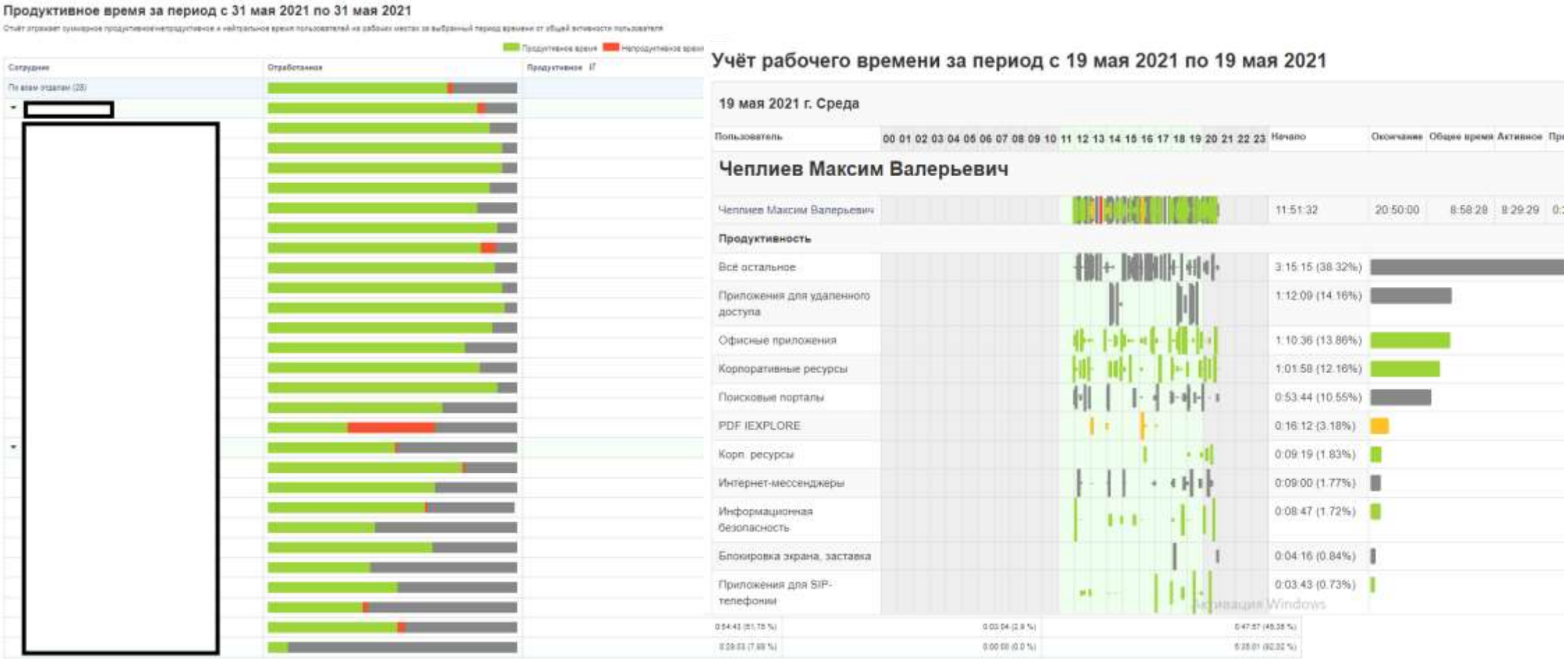
Расследование инцидентов ИБ

- 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

Точность – анализ и формирование конкретных задач



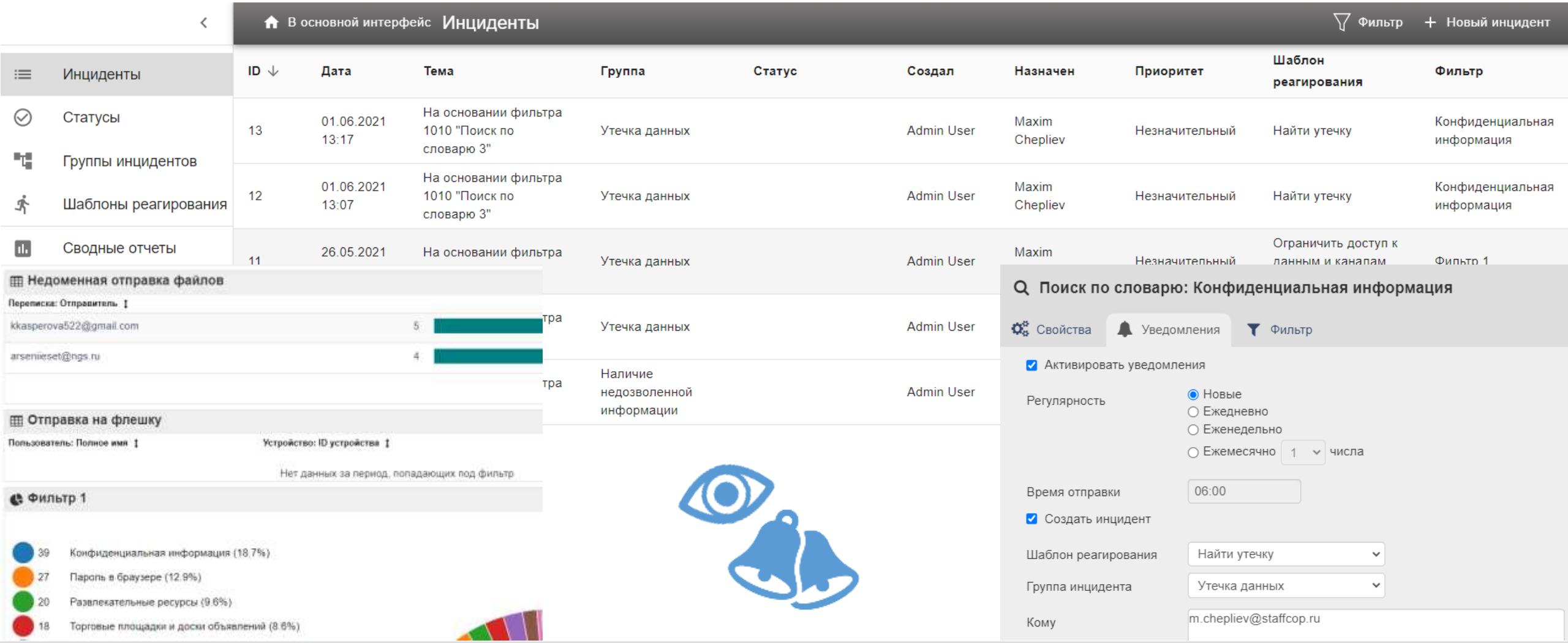
Люди – один из наиболее ценных ресурсов.



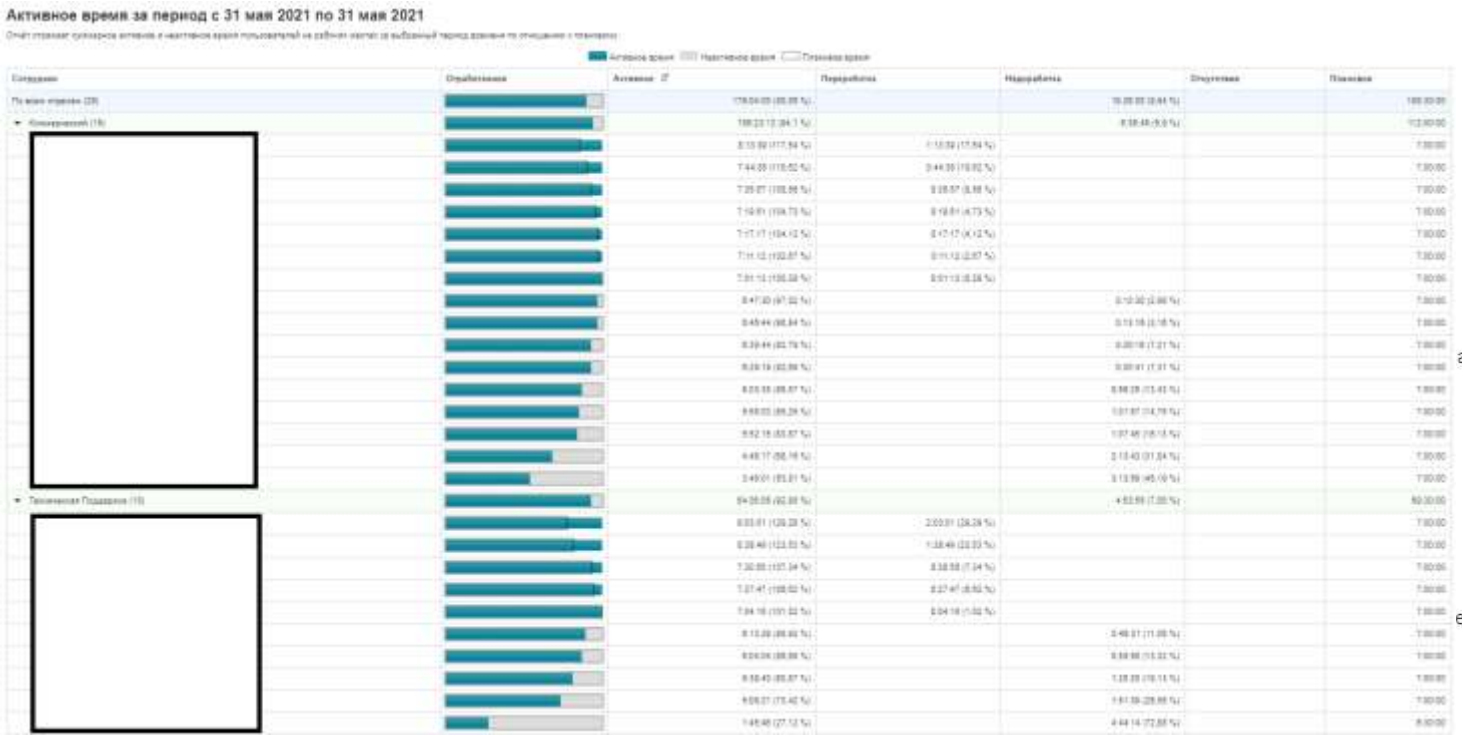
Контроль процессов и технологий.

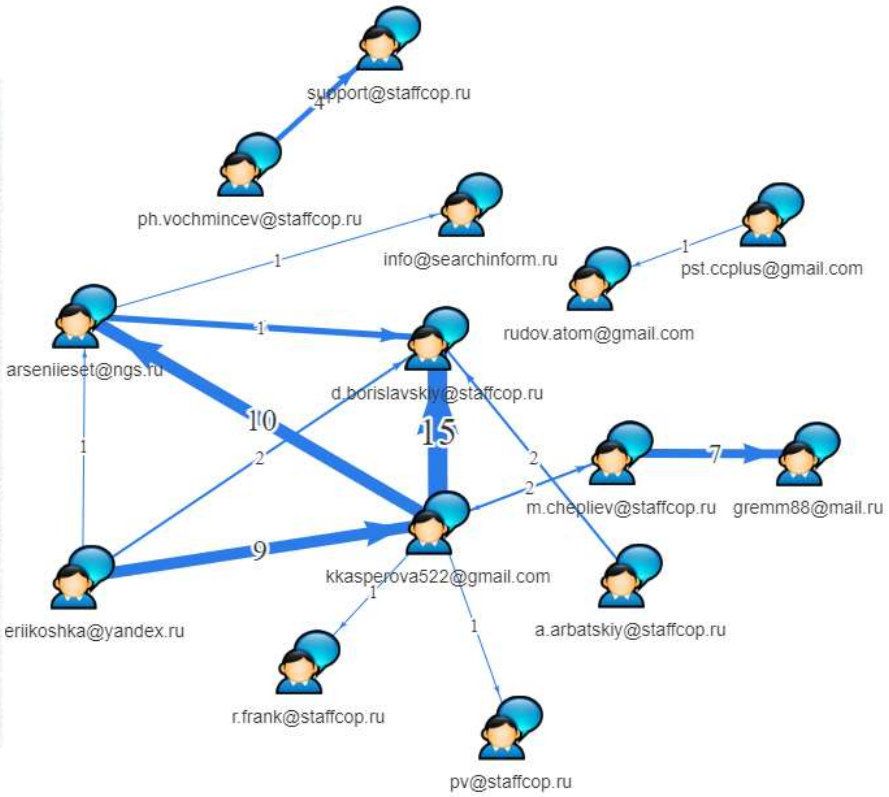
- Мониторинг
- Блокировки
- Инвентаризация ПО и «железа»
- Уровни доступа к данным и функционалу в системе
- Интеграция с SIEM

Процесс внедрения, создание точек контроля, уведомлений и организация.

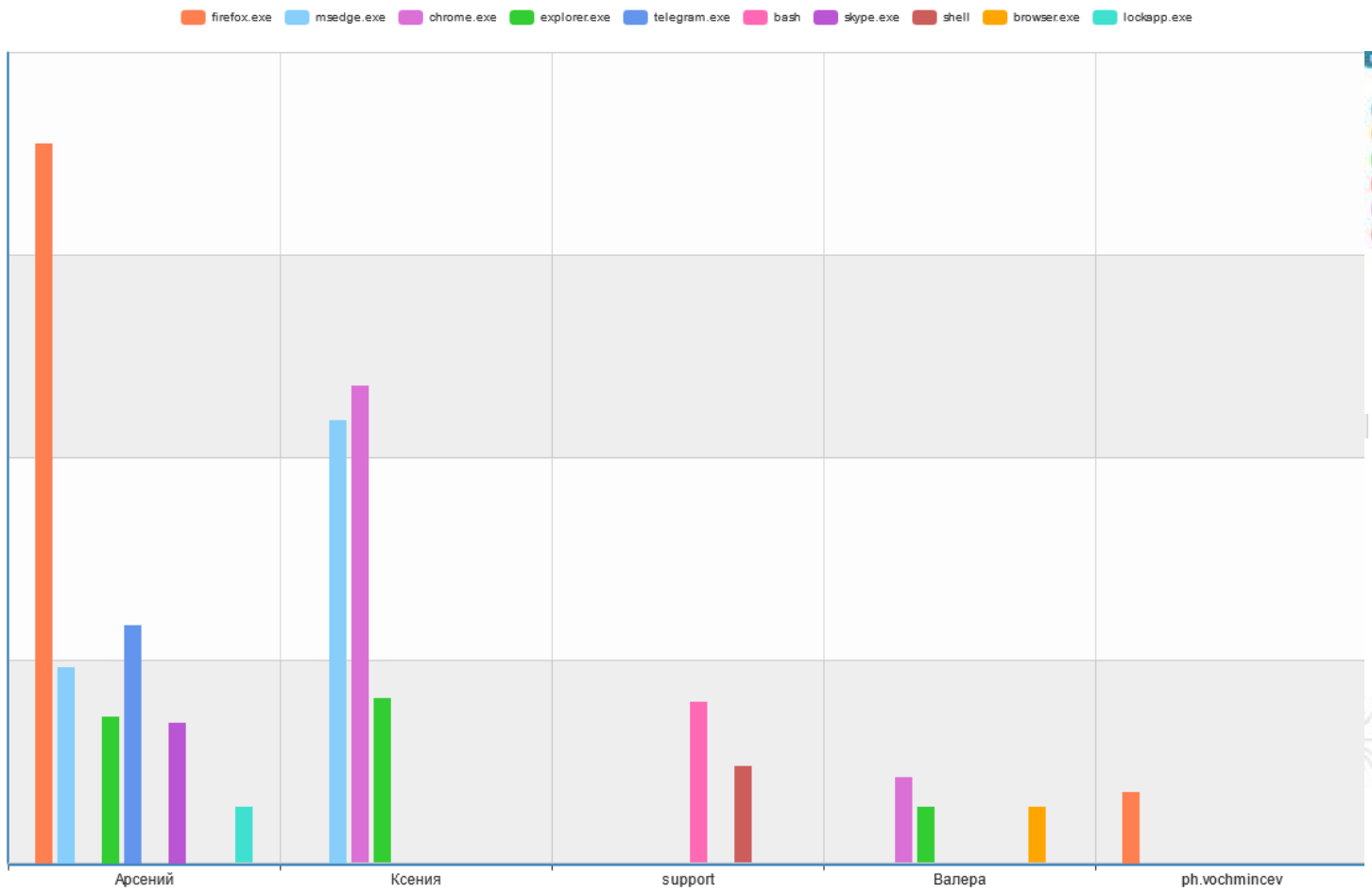


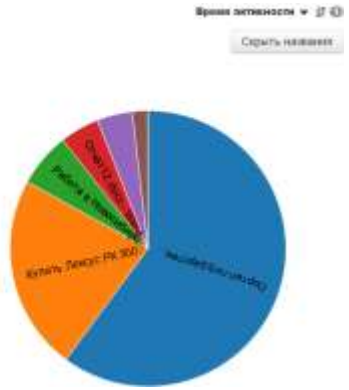
Человек

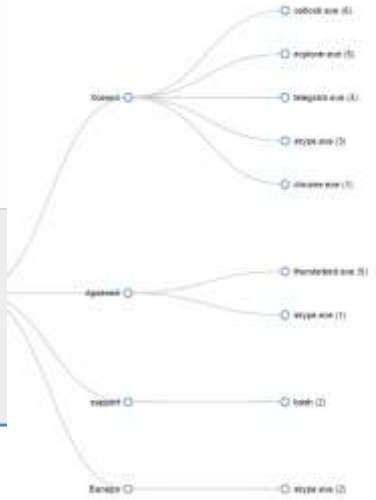

Активное время за период с 31 мая 2021 по 31 мая 2021


support@staffcop.ru
ph.vochmincev@staffcop.ru
info@searchinform.ru
pst.ccplus@gmail.com
rudov.atom@gmail.com
arseniieset@ngs.ru
d.borislavskiy@staffcop.ru
m.chepliev@staffcop.ru
gremm88@mail.ru
kkasperova522@gmail.com
eriikoshka@yandex.ru
a.arbatskiy@staffcop.ru
r.frank@staffcop.ru
pv@staffcop.ru

Человек и процессы







Человек и технологии

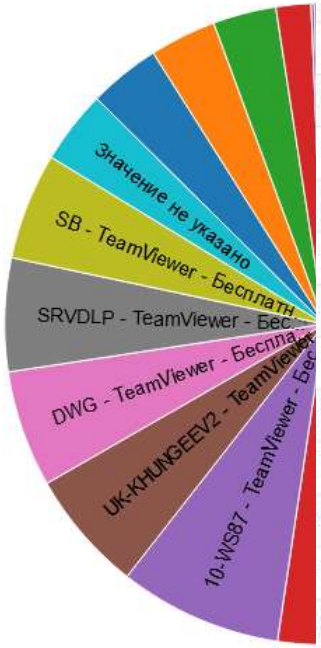
2021-06-21 12:51:22	enterprise	Удаление приложения	libnginx-mod-http-xslt-filter
2021-06-21 12:51:22	enterprise	Удаление приложения	ufw
2021-06-21 12:51:22	enterprise	Удаление приложения	isc-dhcp-common
2021-06-21 12:51:22	enterprise	Удаление приложения	install-info
2021-06-21 12:51:22	enterprise	Удаление приложения	apport
2021-06-21 12:51:22	enterprise	Установка приложения	liblz4-1:amd64
2021-06-21 12:51:22	enterprise	Удаление приложения	nginx-common
2021-06-21 12:51:22	enterprise		
2021-06-21 12:51:22	enterprise		
2021-06-21 12:51:22	enterprise		
2021-06-21 12:51:22	enterprise		
2021-06-21 12:51:22	enterprise		

Инвентаризация - Устройства

Статус	Компьютер	Производитель	Тип устройства	HWID	Дата наличия
Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IKEv2)	SWD\MSRRAS\MS_AGILEVPNMI	17:50:00 09.07.2021
Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IPv6)	SWD\MSRRAS\MS_NDISWANIPv	17:50:00 09.07.2021
Добавлено	Arsenii	GenuineIntel	CPU: Intel(R) Xeon(R) CPU E5-2470 v2 @ 2.40GHz	CPU0	17:50:00 09.07.2021
Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (Network Monitor)	SWD\MSRRAS\MS_NDISWANBH	17:50:00 09.07.2021
Добавлено	Arsenii		Printer: Fax		17:50:00 09.07.2021
Добавлено	Arsenii	(Standard system devices)	Mouse: USB Input Device	USB\VID_0E0F&PID_0003&MI_0	17:50:00 09.07.2021
Добавлено	Arsenii	Microsoft	Mouse: PS/2 Compatible Mouse	ACPI\VMW0003\4&1BD7F811&0	17:50:00 09.07.2021
Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IP)	SWD\MSRRAS\MS_NDISWANIP	17:50:00 09.07.2021
Добавлено	Arsenii	(Standard disk drives)	Disk Drive: VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PRC	17:50:00 09.07.2021

Процессы и технологии

177	UK-KHUNGEEV - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (14.9%)
121	MSKNOTE454 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (10.2%)
100	DESKTOP-488B60V - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (8.4%)
98	10-WS87 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (8.2%)
73	UK-KHUNGEEV2 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (6.1%)
70	DWG - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (5.9%)
68	SRVDLP - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (5.7%)
64	SB - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (5.4%)
44	Значение не указано (3.7%)
43	Идентификация TeamViewer (3.6%)
40	DESKTOP-00LAFND - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (3.4%)
38	MKS15 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (3.2%)
21	Спонсируемый сеанс (1.8%)
2	Version out-of-date: Update the remote TeamViewer (0.2%)
2	201 952 415 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (0.2%)
2	HQ-WS-0526 - TeamViewer - Бесплатная лицензия (только некоммерческое использование) (0.2%)



СИСТЕМА		
Ксения	Удаление	25
Арсений	Создание	15
Ксения	Копирование	14
Арсений	Копирование	12
Валера	Создание	8
Ксения	Перезапись	8
Ксения	Удаление	5
Ксения	Подключение	4
Ксения	Запись	3
Ксения	Переименование	3
Валера	Создание	3
Валера	Переименование	3
Арсений	Запись	3
Валера	Копирование	2
Арсений	Переименование	2
Ксения	Перемещение	1
Валера	Подключение	1
Валера	Запись	1

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

Политика лицензирования и стоимость

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

Бессрочная лицензия – по запросу

Благодарю за внимание!

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность

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