



Контроль информационных потоков и рабочих процессов.

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, ~70 сотрудников.
- Продано ~1300 серверных компонентов, ~ 66 000 АРМ за 2019-й год.
- Продано ~2200 серверных компонентов, ~ 171 000 АРМ за 2020-й год.
- Продано ~3100 серверных компонентов, ~ 230 000 АРМ за 2021-й год.



Зачем это все нужно?

Инциденты

- Что случилось?
- Как это произошло?

Люди

- Как сотрудники работают в офисе и на удаленке?
- С чем они работают?
- Как настроения?

Информация

- Кто имеет к ней доступ?
- Как с ней работают?
- Какое ПО используют

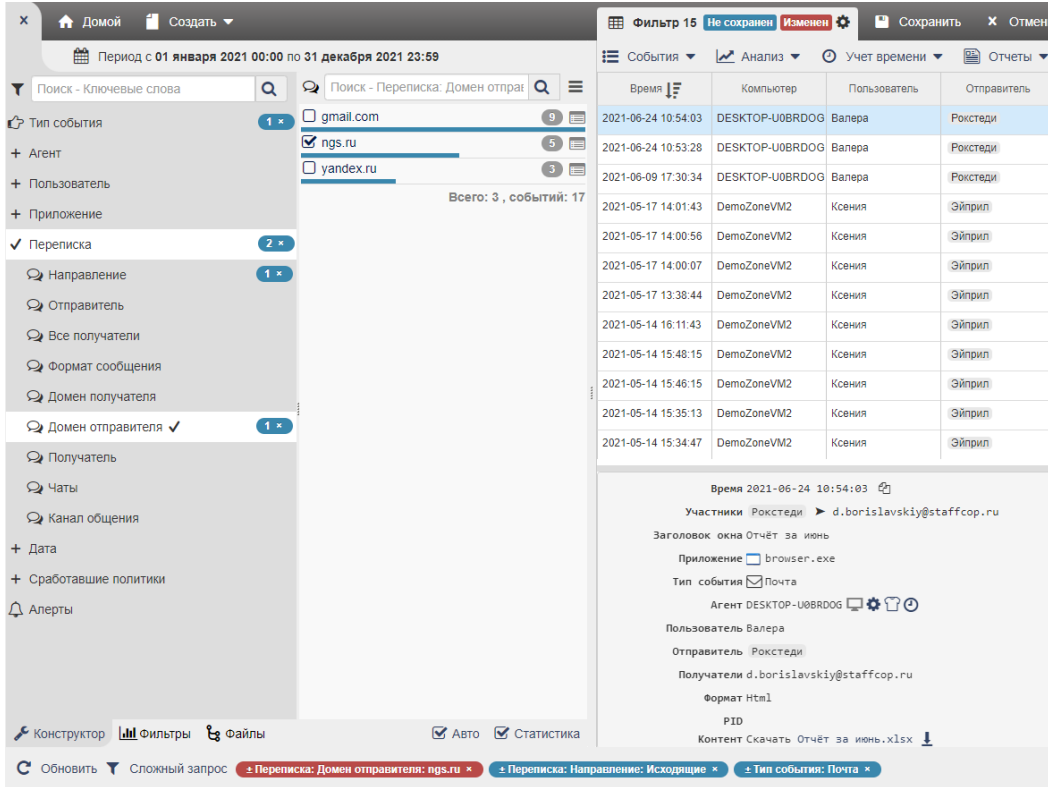
Контроль распространения информации

- Преднамеренные и непреднамеренные утечки
- Конфиденциальная информация, Персональные данные
- Переписка внутренняя и внешняя, мессенджеры
- Каналы утечки

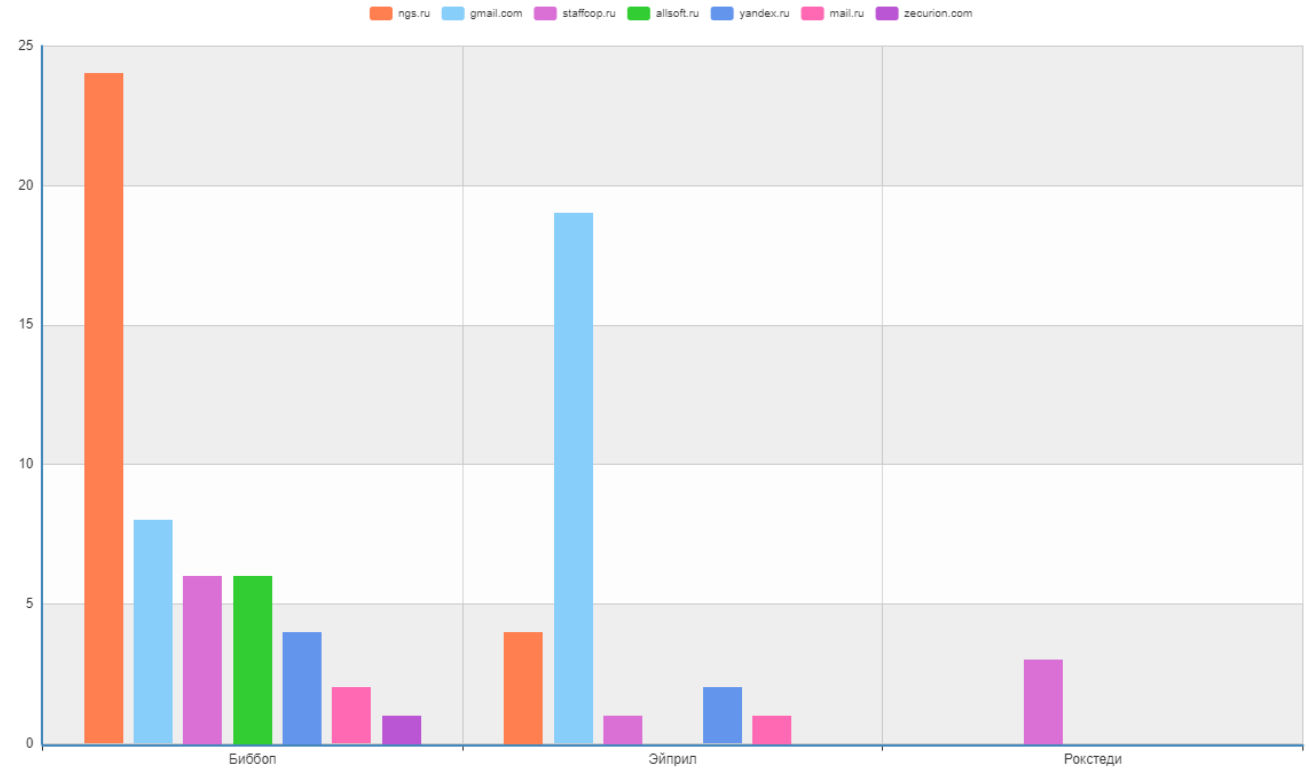
Нерегламентированная и опасная деятельность

- Установка опасного ПО и работа в portable приложениях.
- Посещение опасных и вредоносных ресурсов
- Ссылки в письмах
- Переписка с использованием личной почты

Задачи для бизнеса



Скриншот интерфейса STAFFCOP. В центре — таблица событий с колонками: Время, Компьютер, Пользователь, Отправитель. Внизу — подробная информация о событии: время, участники, приложение (browser.exe), тип события (Почта), агент (DESKTOP-U0BRDOG), пользователь (Валера), отправитель (Рокстеди), получатели (d.borislavskiy@staffcop.ru), формат (Html), PID.



Всего: 4, Количество событий: 42

Пользователь: Полное имя	Переписка: Канал общения	Количество событий
Эйприл	Mail	14
Эйприл	Telegram	14
Биббон	Mail	9
Рокстеди	Mail	5

Деструктивное поведение и характеристика сотрудников

- Поиск работы и подготовка к увольнению
- «Нерабочие» отношения, конфликты
- Поиск правых и виноватых
- Характеристика сотрудников

Неэффективные рабочие процессы

- «Леваки»
- Халатное отношение к работе и «пожиратели» рабочего времени
- Неравномерная нагрузка
- Неверно настроенные бизнес-процессы, коммуникации.

Флешка


Пользователь: Полное имя | Устройство: ID устройства |

[Эйприл](#) | USBVID_090C&PID_1000V0113000000000602 | 6

Всего: 1, Количество событий: 6
Количество событий | 1

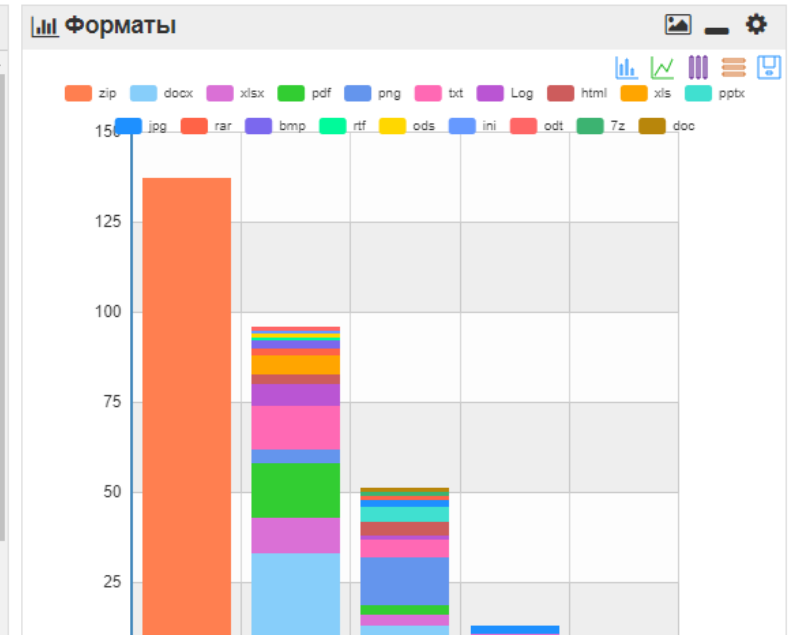
Почта

Скругление | Визуализация | Кнопки навигации



Договора

Время	Компьютер	Пользователь	Приложение	Получатели
2021-07-2	Arsenii	Арсений	thund	d.borislavskiy@sta
2021-07-2	Arsenii	Арсений	thund	Биббон
2021-05-2	DemoZor	Ксения	skype	8:live:..cid.478d16
2021-05-2	DemoZor	Ксения	skype	8:live:..cid.478d16



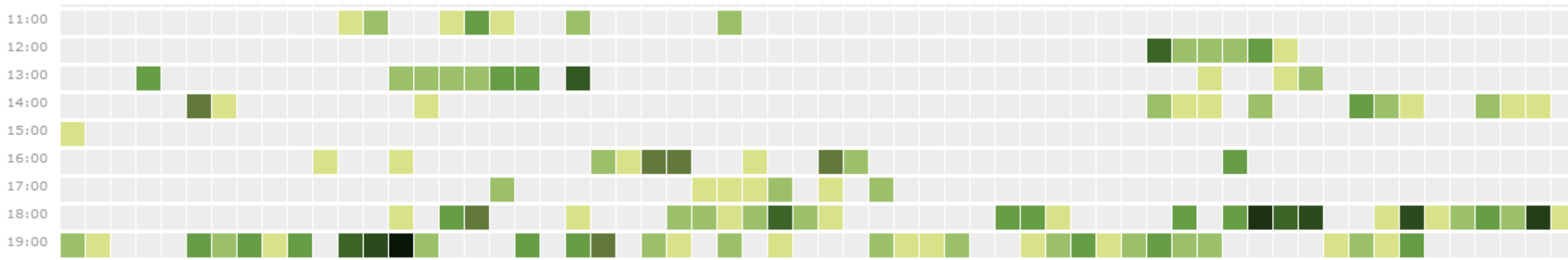
Деструктивное поведение и характеристика сотрудников

- Поиск работы и подготовка к увольнению
- «Нерабочие» отношения, конфликты
- Поиск правых и виноватых
- Характеристика сотрудников

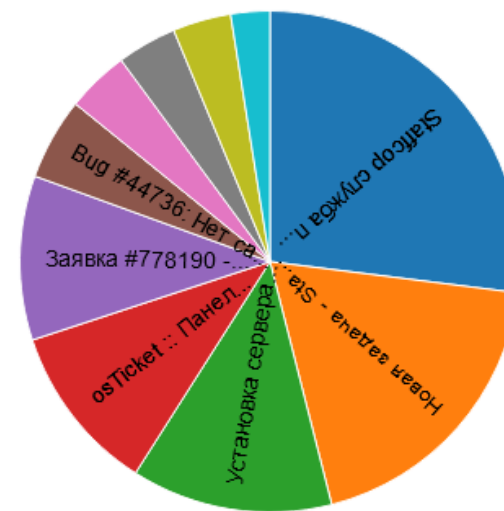
Неэффективные рабочие процессы

- «Леваки»
- Халатное отношение к работе и «пожиратели» рабочего времени
- Неравномерная нагрузка
- Неверно настроенные бизнес-процессы, коммуникации.

Задачи для бизнеса



- 00 ч 13 м 53 с Staffcop служба поддержки клиентов - Google Chrome (27%)
- 00 ч 09 м 48 с Новая задача - Staffcop Enterprise - Atom Security - Google Chrome (19%)
- 00 ч 08 м 42 с Установка сервера распознавания графических объектов — документация Staffcop Enterprise 4.9 - Google Chrome (13%)
- 00 ч 05 м 37 с osTicket :: Панель управления персонала - Google Chrome (10.9%)
- 00 ч 05 м 27 с Заявка #778190 - Google Chrome (10.6%)
- 00 ч 02 м 44 с Bug #44736: Нет сайтов во времени активности в opera и firefox на агентах 2542 - Staffcop Enterprise - Atom Security - Google Chrome (5.3%)
- 00 ч 02 м 05 с Поиск - Atom Security - Google Chrome (4%)
- 00 ч 01 м 59 с Atom Security - Google Chrome (3.9%)
- 00 ч 01 м 57 с Заявка #348145 - Google Chrome (3.8%)
- 00 ч 01 м 18 с Руководство администратора — документация Staffcop Enterprise 4.9 - Google Chrome (2.5%)



Инвентаризация и администрирование

- Контроль лицензионного и нерегламентированного ПО
- «Потеря» оперативной памяти
- Удаленное подключение для помощи сотруднику

Уникальные задачи

- Переговоры и взаимодействие с клиентами
- Компьютер в «общем» доступе
- Политика чистых столов

Задачи для бизнеса

Период с 16 августа 2021 00:00 по 14 сентября 2021 23:59

Поиск - Ключевые слова

Поиск - Агент: Компьютер

Тип события 1 x

Агент 1 x

IP адрес

Группа

Сотрудник

Компьютер ✓ 1 x

Статус

Версия OS

Версия агента

Пользователь

Дата

Сработавшие политики

Алерты

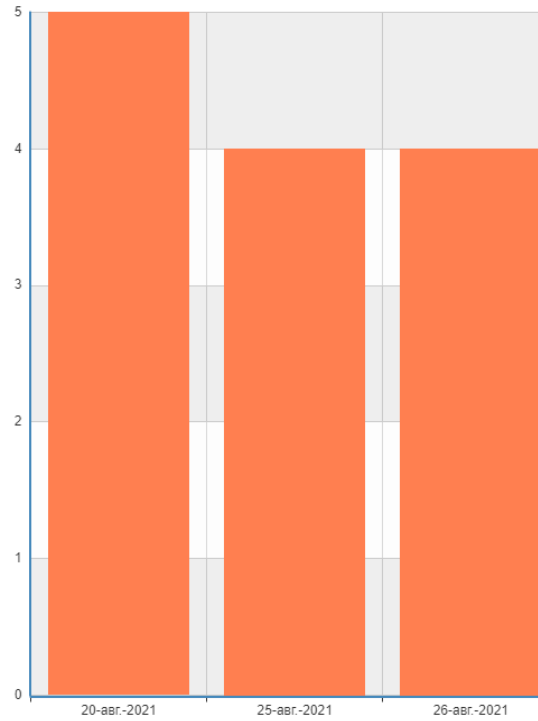
Всего: 7, событий: 165

Конструктор | Фильтры | Файлы | Авто | Статистика

Обновить | Сложный запрос | Агент: Компьютер: DESKTOP-U0BRDOG | Тип события: Вход/выход из системы

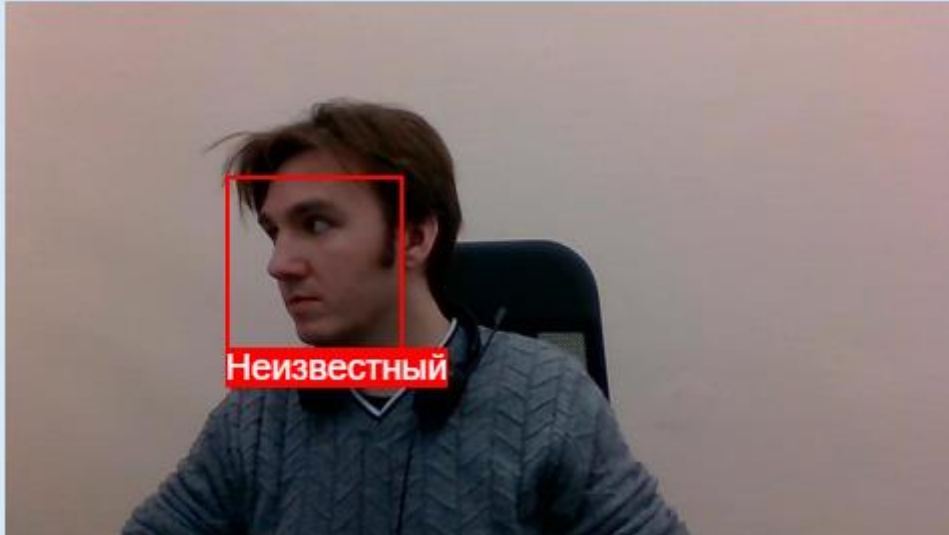
События | Анализ | Учет времени | Отчеты

Дата: День



Дата	Кол-во
20-avg-2021	5
25-avg-2021	4
26-avg-2021	4

Неизвестное лицо



Топ опоздавших	Кол-во
Рафаэль	3
Леонардо	3
Микеланджело	3
Донателло	2
Эйприл	1

Топ по времени опозданий	Кол-во
Микеланджело	5ч 46м 55с
Эйприл	5ч 27м 27с
Леонардо	2ч 15м 05с
Рафаэль	1ч 59м 20с
Донателло	30м 55с



Система мониторинга для расследования инцидентов
и контроля работы сотрудников



Учет рабочего
времени



Эффективность
персонала



Информационная
безопасность



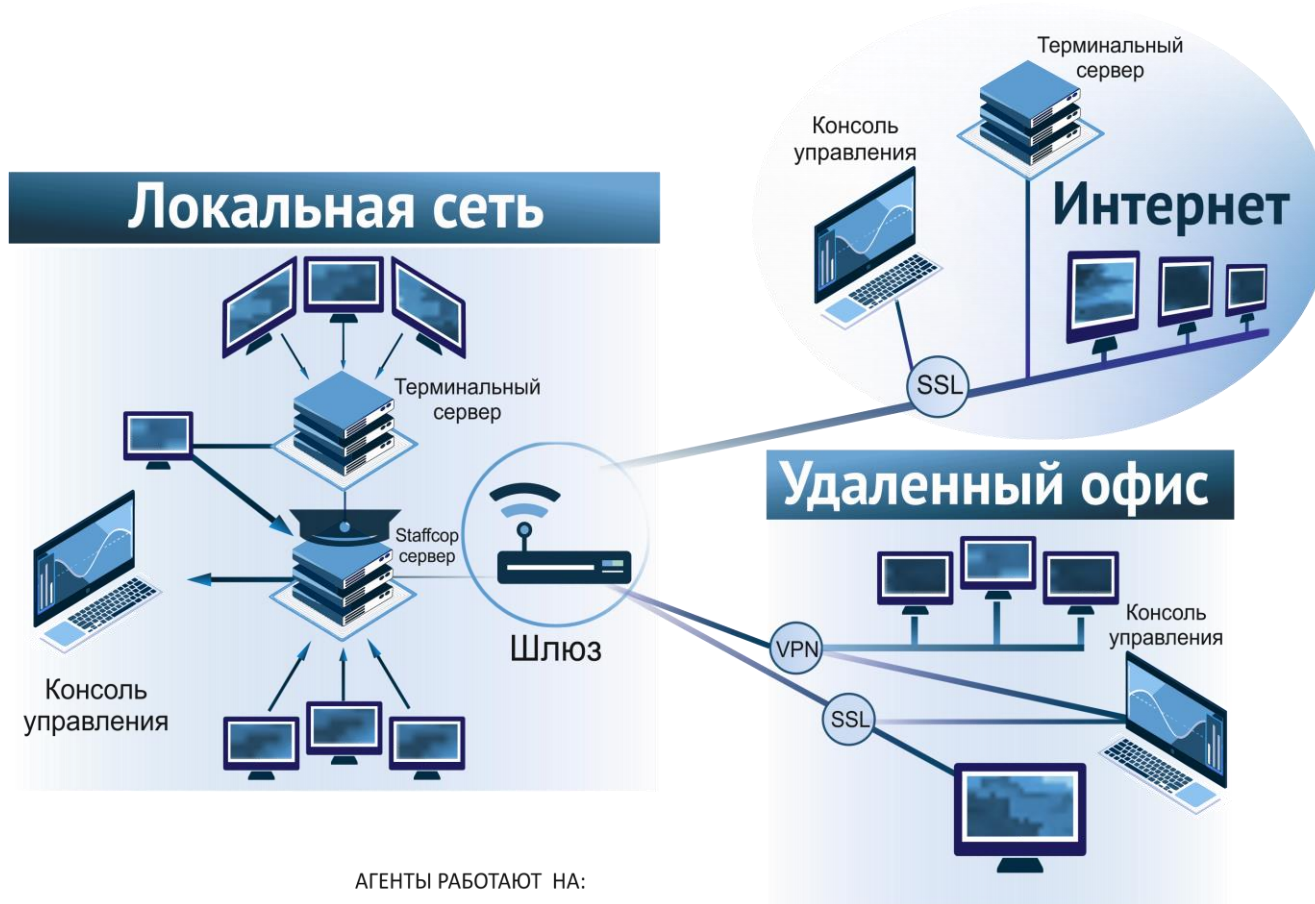
Расследование и
инцидентов



Удаленное
администрирование

Как это работает?

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

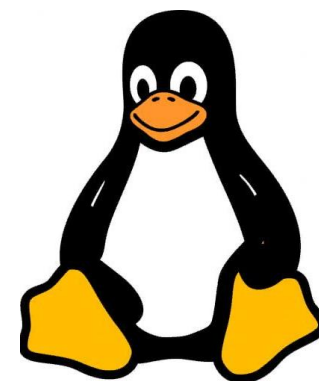
Множество способов установки агентов, как локальные, так и удаленные.

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

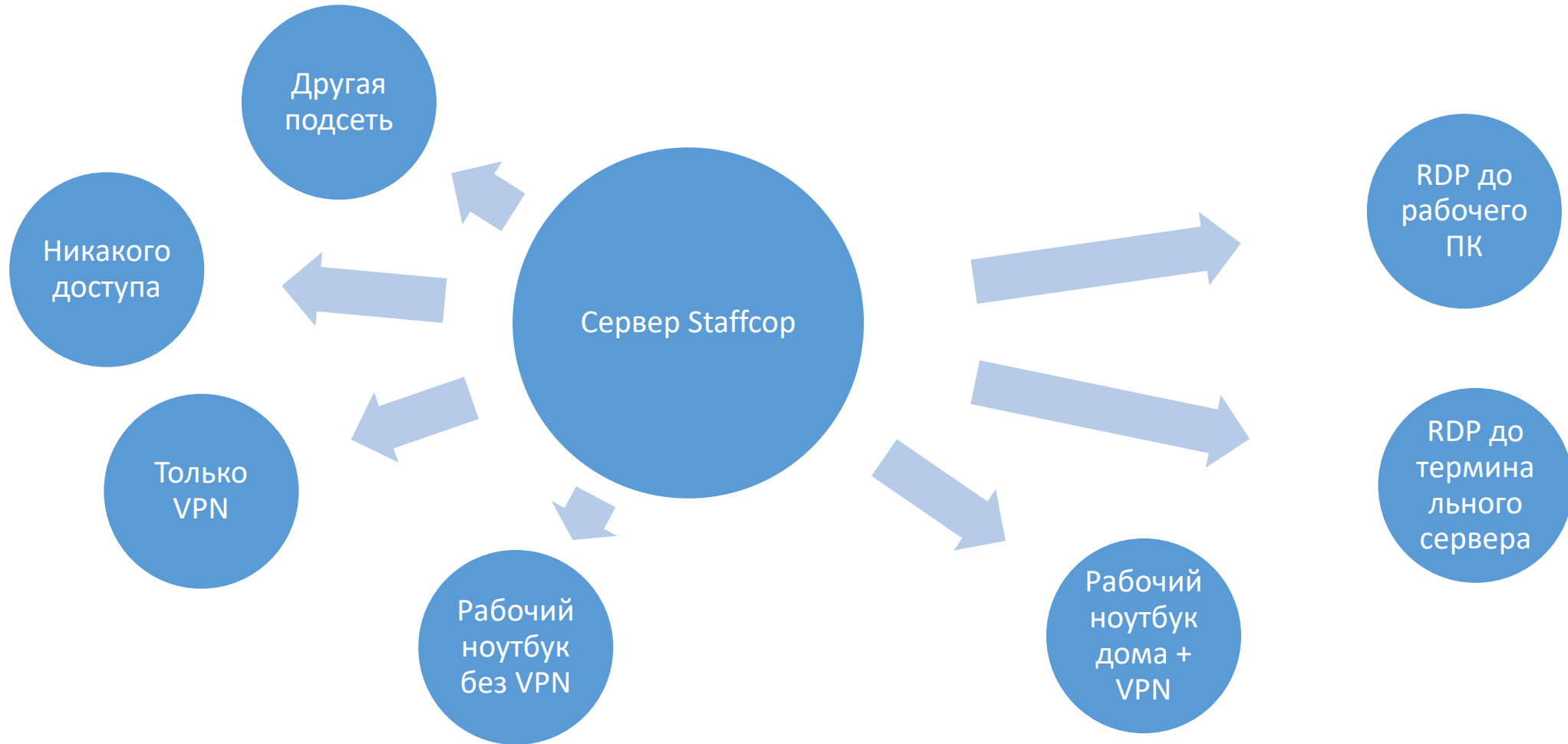
- Технологии сервера:



OS рабочих ПК и АРМ:



Кого можно контролировать?



Что можно контролировать?

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.

Что можно сделать с помощью нашей системы?

- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений
- Гибкая система настройки фильтров



Преимущества Staffcop Enterprise



На opensource решениях, не требует дополнительного платного ПО.



Цена.



Входим в реестр отечественного ПО и имеет сертификат ФСТЭК.



Небольшие требования к ресурсам для сервера. Единая web-консоль.



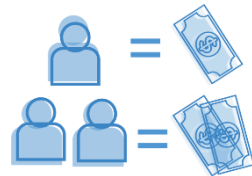
Настраиваемые отчёты и OLAP.



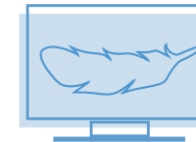
Не блокирует работу бизнеса.



Решает задачи разных подразделений



Единое решение и гибкая политика лицензирования.



Лёгкий и функциональный агент.

Количество компьютеров	Лицензия на 12 месяцев	Лицензия на 3 месяца
5–25	3 350 ₽ / 1 ПК	1 117 ₽ / 1 ПК
26–50	3 150 ₽ / 1 ПК	1 050 ₽ / 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		

Тестируйте бесплатно на парке АРМ любого размера.

Полнофункциональная версия.

Техническое сопровождение проекта на всём протяжении тестирования.



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
Принять правильное
решение

Чеплиёв Максим

Ведущий специалист отдела внедрения
ООО Атом Безопасность

 +7(499)6382809 доб. 238

 m.chepliev@staffcop.ru