Контроль информационных потоков – комплексное обеспечение информационной безопасности при удаленной рабочей деятельности.

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

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

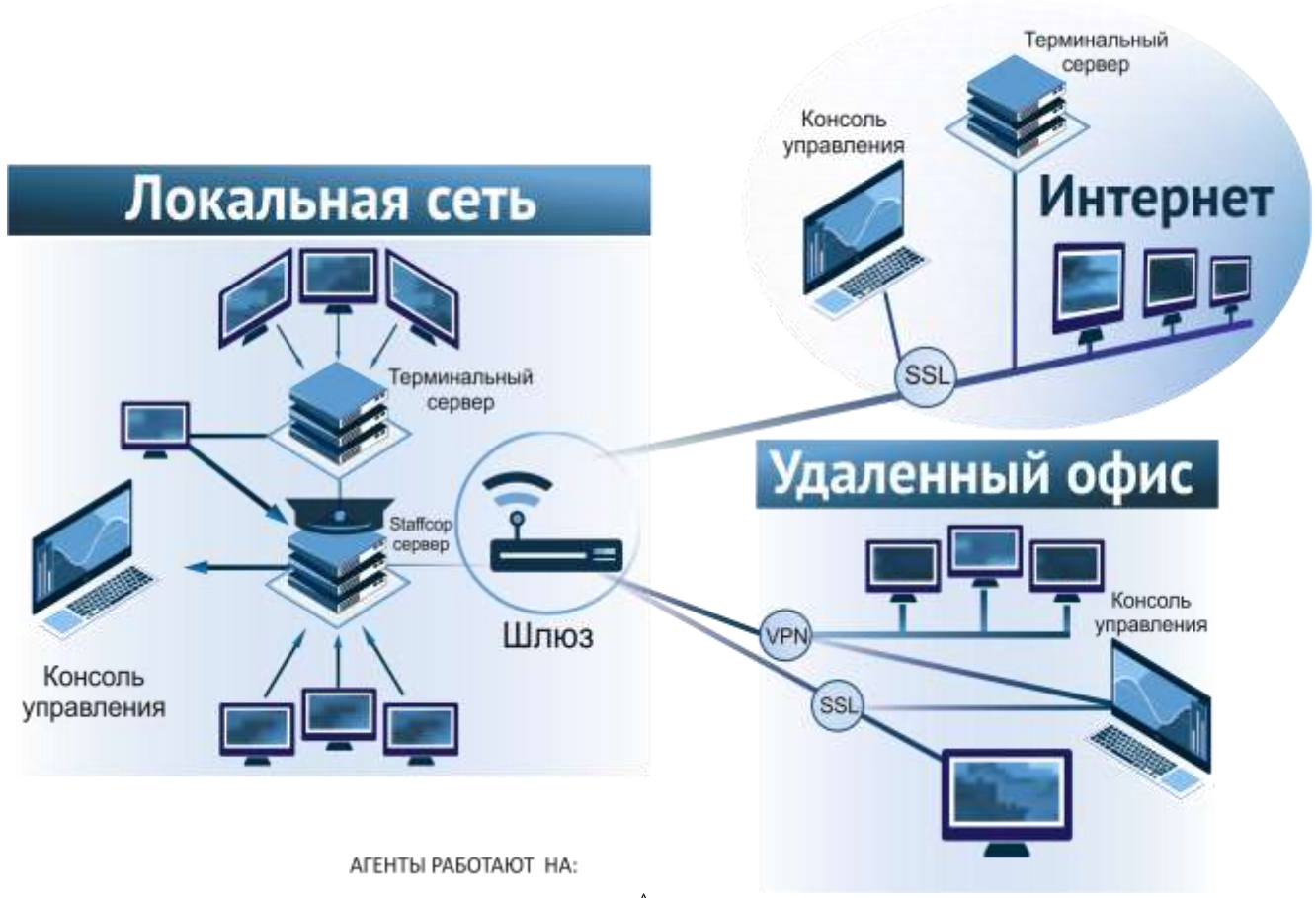
- Обеспечение контроля взаимодействия
- Доступ к информации
- Передача информации

Аутентификация

- Контроль надежности доступа.
- Контроль доступа к учетной записи

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

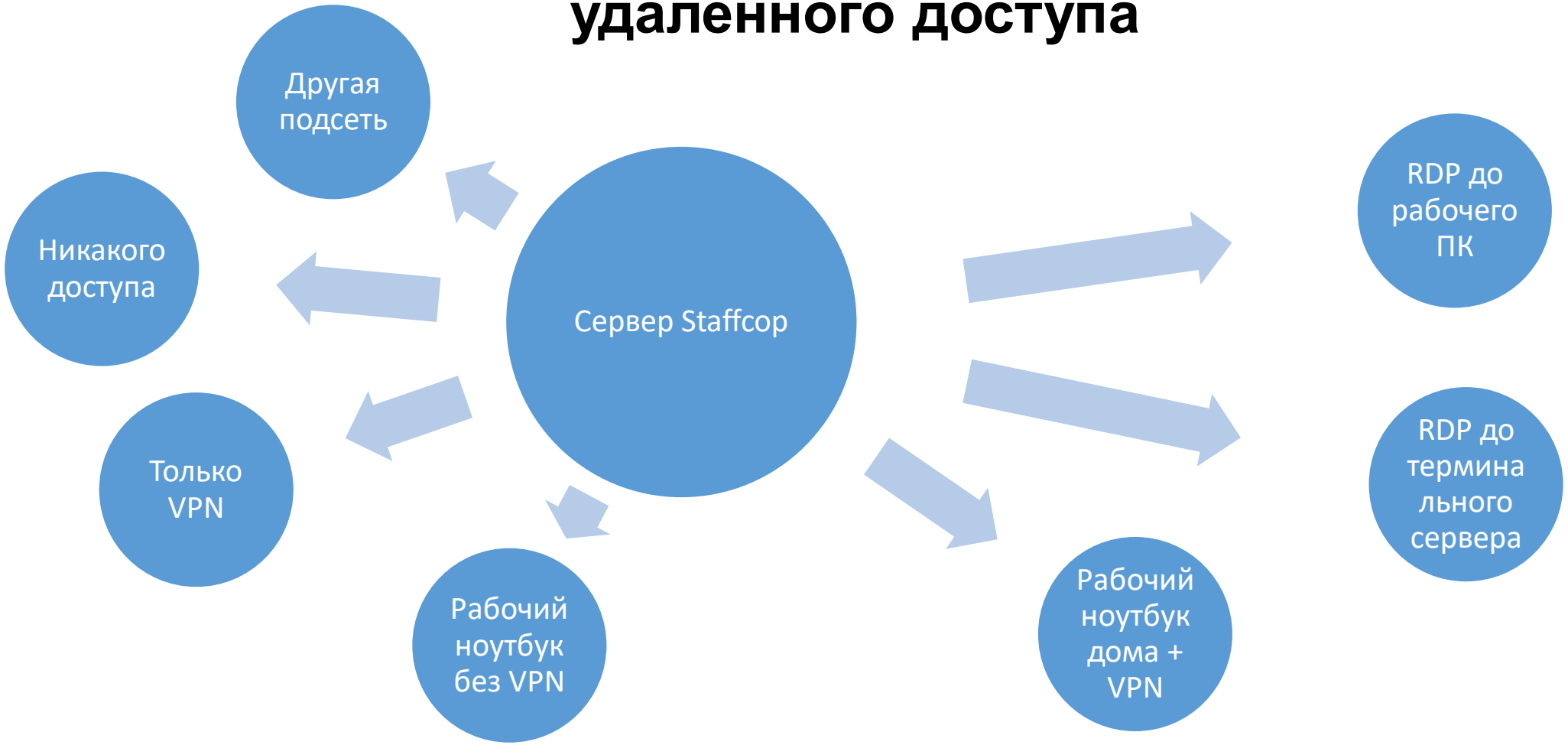
Перехват сообщений в мессенджерах

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.

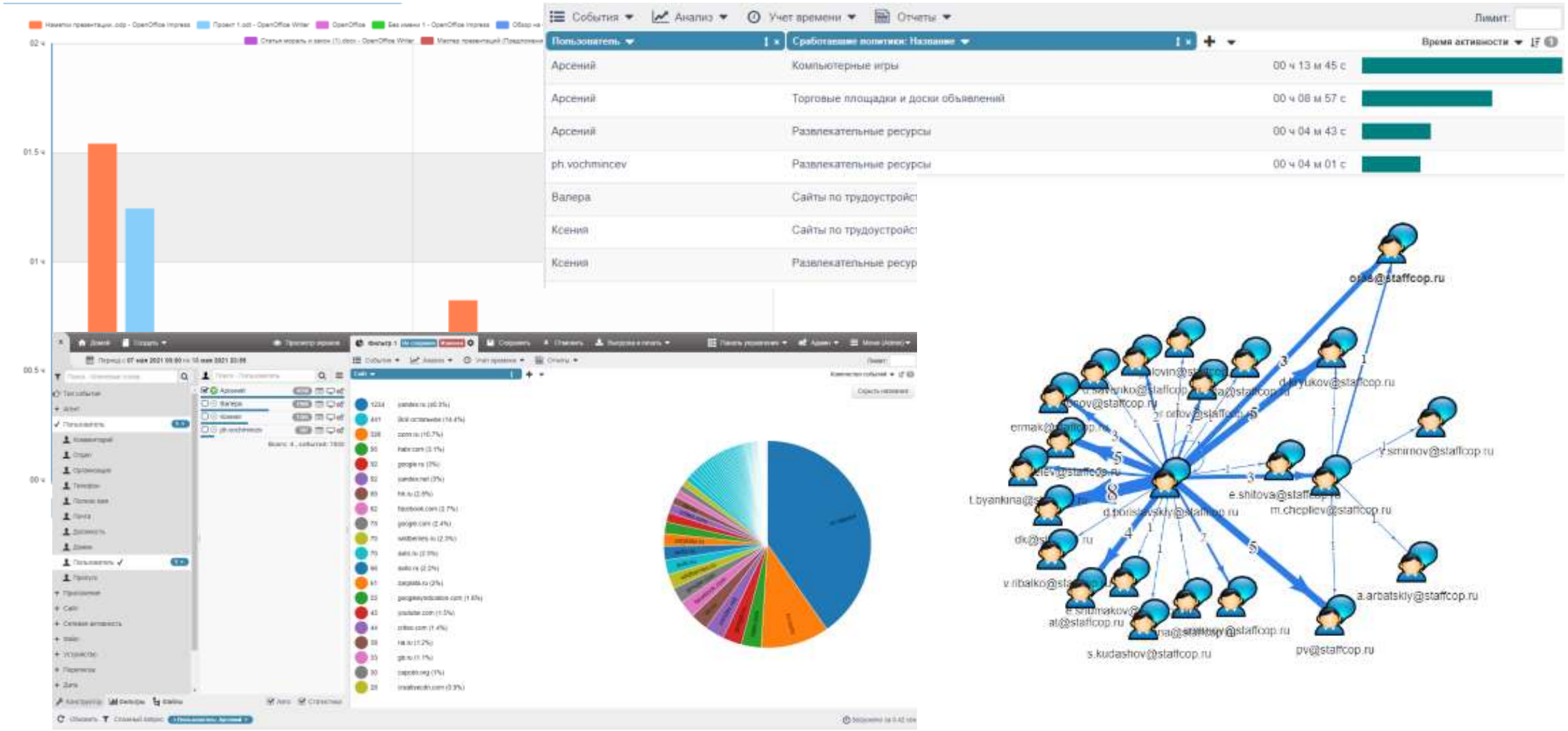
Контроль рабочих процессов осуществляющихся посредством удаленного доступа



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

Анализ собранной информации



Организация расследований инцидентов

В основной интерфейс **Инциденты**

Фильтр | + Новый инцидент

- Инциденты
- Статусы
- Группы инцидентов
- Шаблоны реагирования
- Сводные отчеты

ID	Дата	Тема	Группа	Статус	Создал	Назначен	Приоритет	Шаблон реагирования	Фильтр
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
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
11	26.05.2021	На основании фильтра	Утечка данных		Admin User	Maxim	Незначительный	Ограничить доступ к данным и каналам	Фильтр 1
		тра	Утечка данных		Admin User				
		тра	Наличие недозволенной информации		Admin User				

Недоменная отправка файлов

Переписка: Отправитель

kkasperova522@gmail.com	5
arseniieset@ngs.ru	4

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: 06:00

☑ Создать инцидент

Шаблон реагирования: Найти утечку

Группа инцидента: Утечка данных

Кому: m.chepliev@staffcop.ru

Словари, фильтры и политики

Поиск по словарю: Конфиденциальная информация

Свойства | Уведомления | Фильтр

Активировать уведомления

Регулярность: Новые / Ежедневно / Еженедельно / Ежемесячно 1 числа

Время отправки: 06:00

Создать инцидент

Шаблон реагирования: Найти утечку

Группа инцидента: Утечка данных

Сложный запрос | Код фильтра

И | 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: Кредитные карты

Категория: Инцидент

Политика активна

Продолжить выполнение

Применить к новым собы

Применить ко всем собы

Внимание! Включение политик

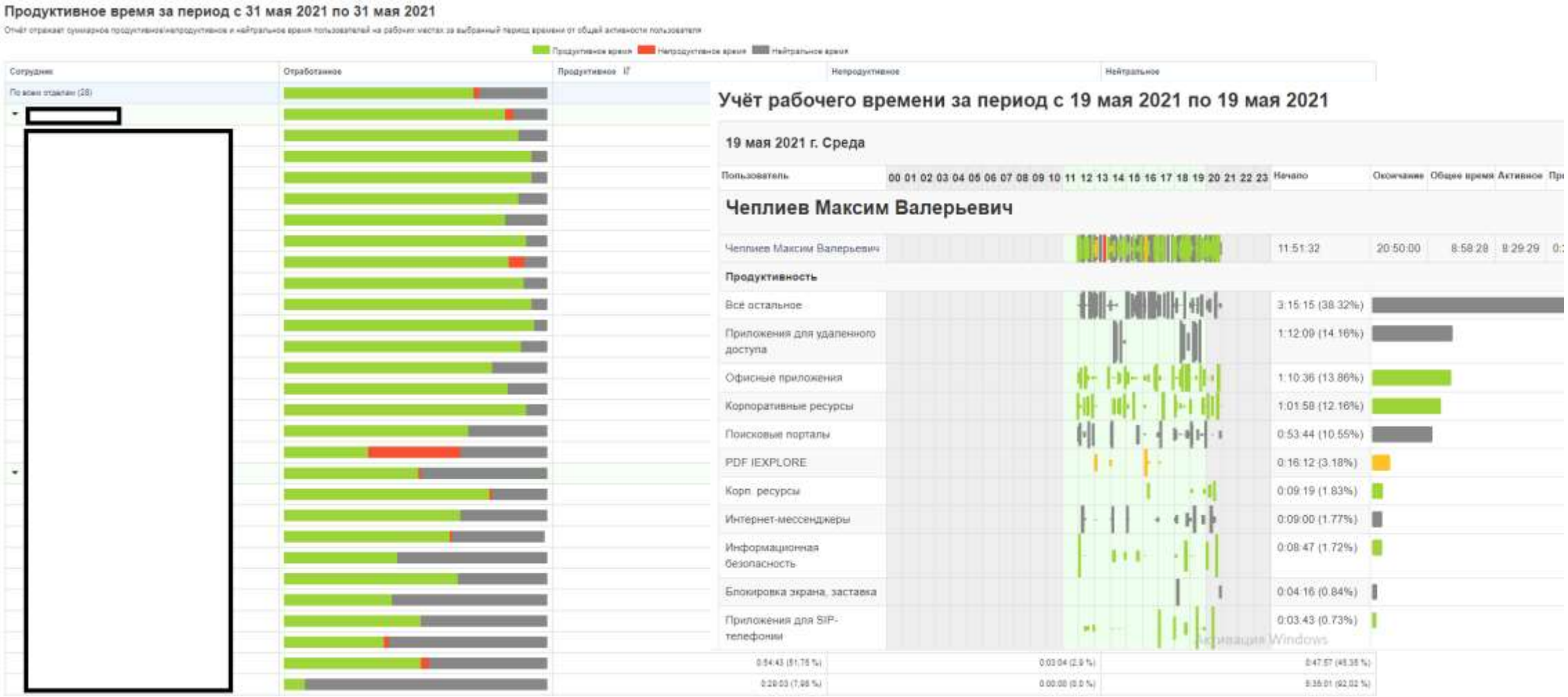
Подсветка найденного:

Словарь:

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

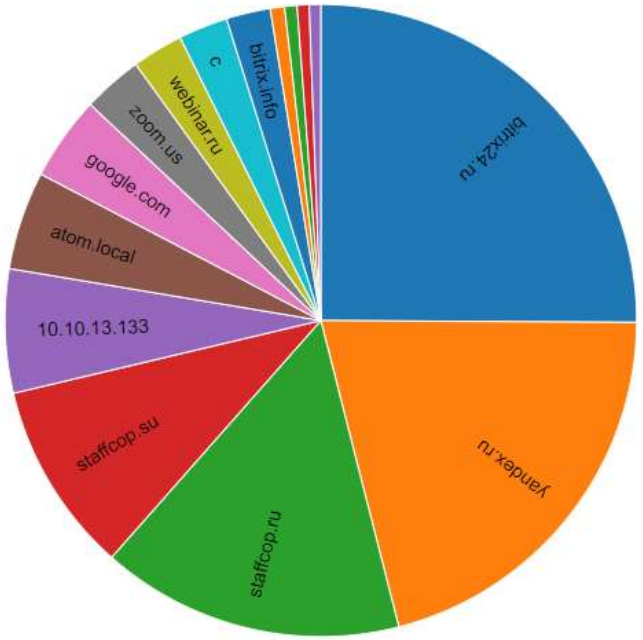
- Политики
  - Политики продуктивности
  - Политики безопасности
    - Словарь ненормативной лексики
    - Словарь наркоманского сленга
    - Словарь откатной тематики
    - Словарь поиска работы
    - Кредитные карты
    - Словарь алкогольной тематики
    - Словарь подарки
    - Словарь долги
    -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

Учет рабочего времени



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

Управление и администрирование

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

Ограничение передачи информации

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:			Удалить правило
Имя пользователя	equals	Ксения	And
And			
Контент	matches	договор × 1234561234 × ИНН ×	And
And			
Имя приложения	equals	outlook.exe	

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

OpenOffice 4.1.9

Доступ к C:\Users\Валера\Documents\Проект 3.odt запрещён.

OK

Блокировка каналов утечки

Правила: Блокировка - Приложения

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

Блокировать

teamviewer.exe

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

userstorage.mega.co.nz/ul/

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

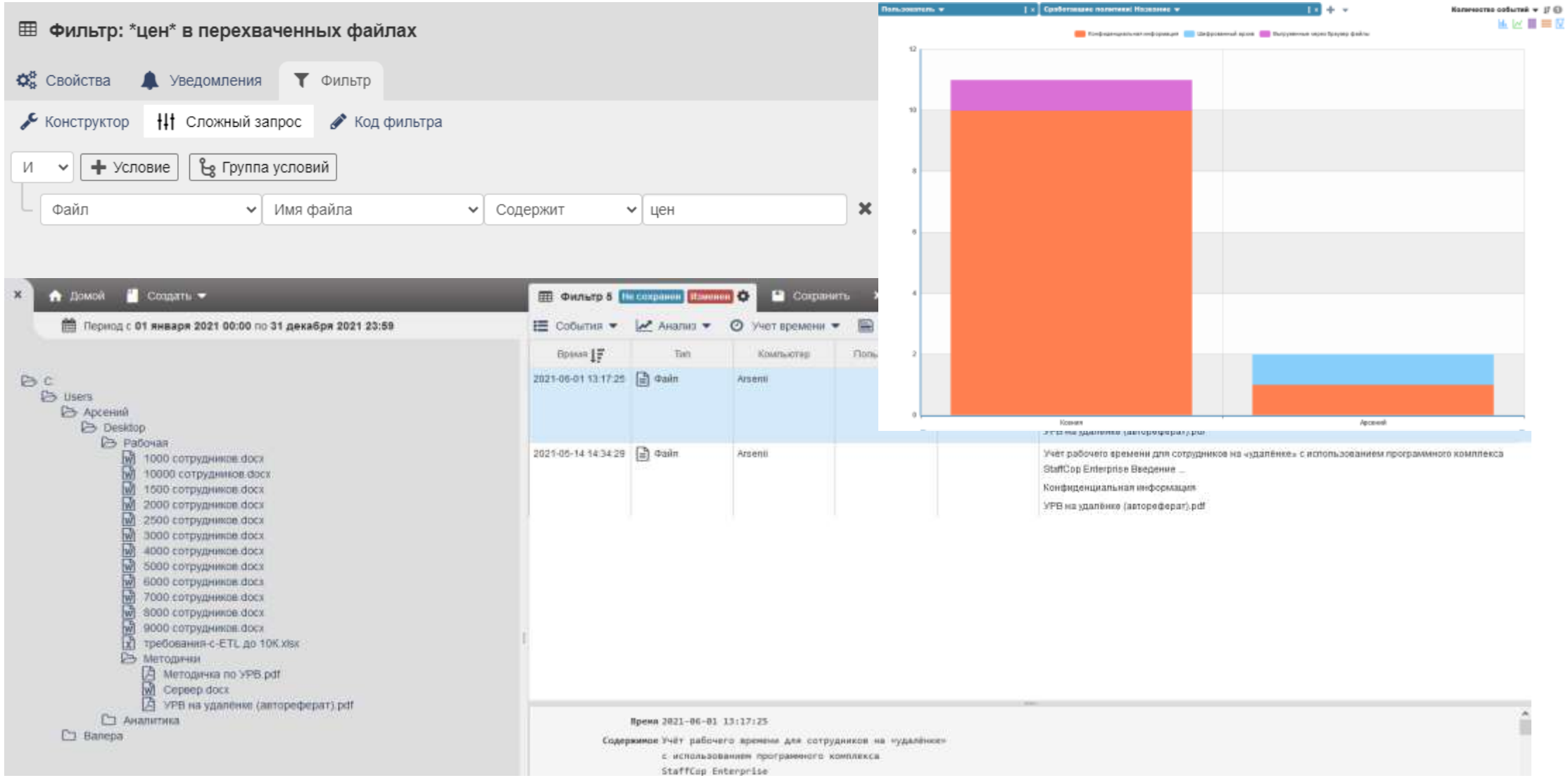
Блокировать - блокировка всех «Device ID» указанных в списке.
Разрешить - блокировка всех «Device ID» за исключением тех, что указаны в данном списке.

Блокировать

Разрешить

USB\VID_090C&PID_1000\0113000000000602

Контроль «владения» информацией

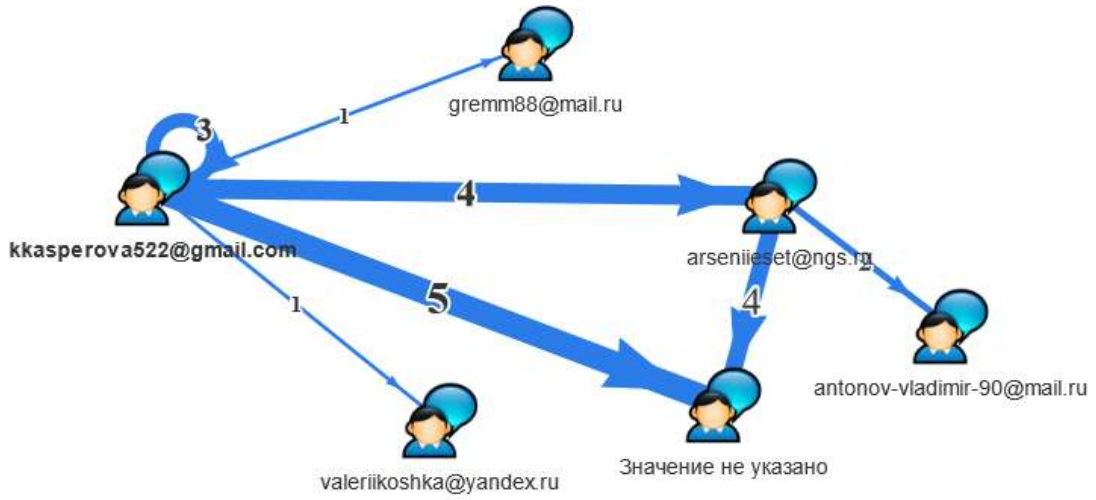


Недоменная переписка, мессенджеры и передача информации конкурентам.

Пользователь	Переписка: Канал общения	Переписка: Отправитель	Количество событий
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	а связи.html	5.2 Kb	Mail
					а связи.html	4.2 Kb	Mail
						184 B	Mail
				-90@mail.ru	Скачать Fwd: сохранитть.html	1.6 Kb	Mail
					Скачать Re: Проверка связи.html	1.4 Kb	Mail
					Скачать Шаблон трудового договора.zip	17.2 Kb	Mail
					Скачать staffc.html	1.7 Kb	Mail

Пользователь	Полное имя	Адрес
		Maxim_Chepliev_79232470277
		kkasperova522@gmail.com
		arseniieset@ngs.ru



Нерегламентированноее 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

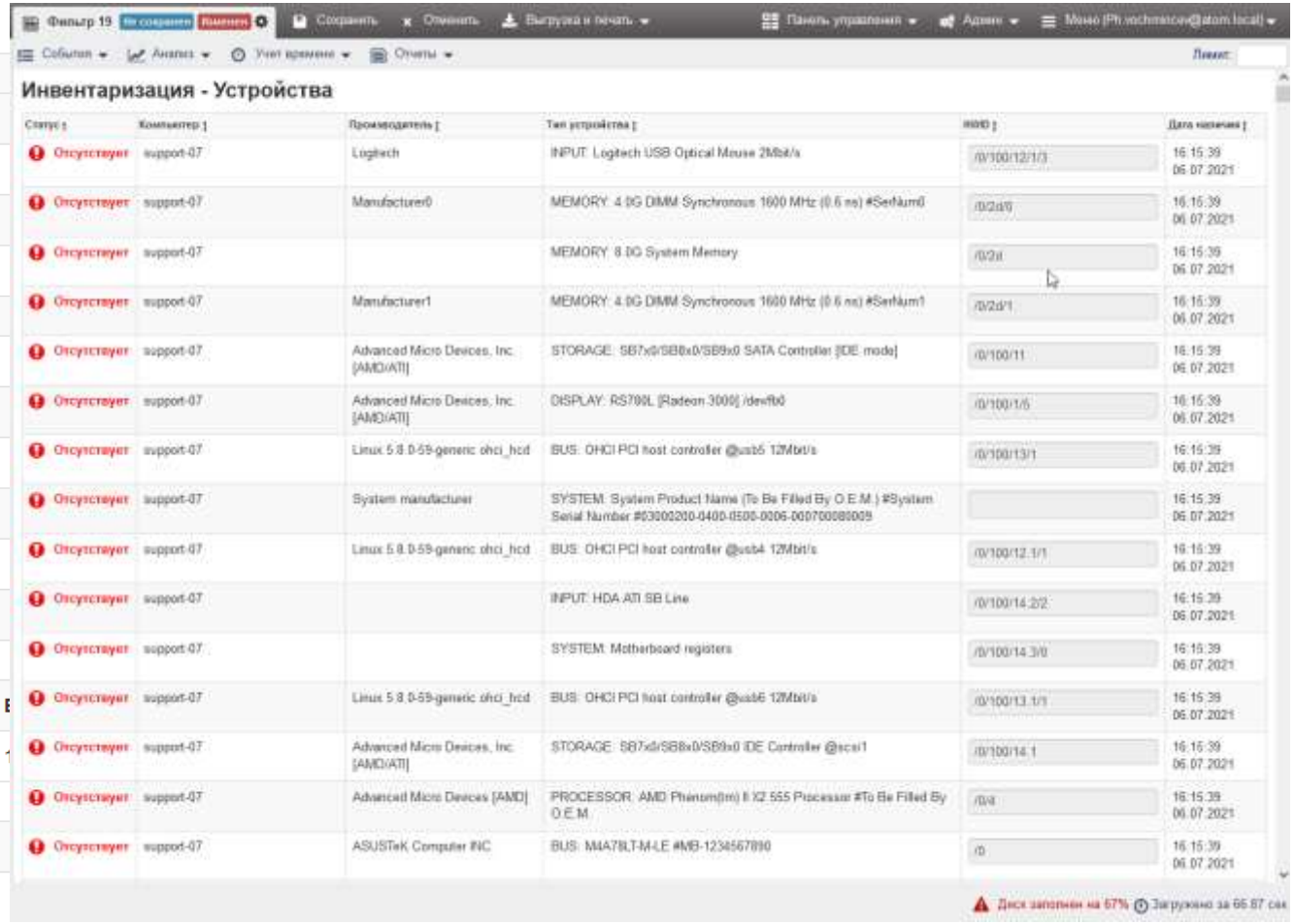
+ Update for Microsoft Office 2016 (KB4011225) 32-Bit Edition

— TeamViewer

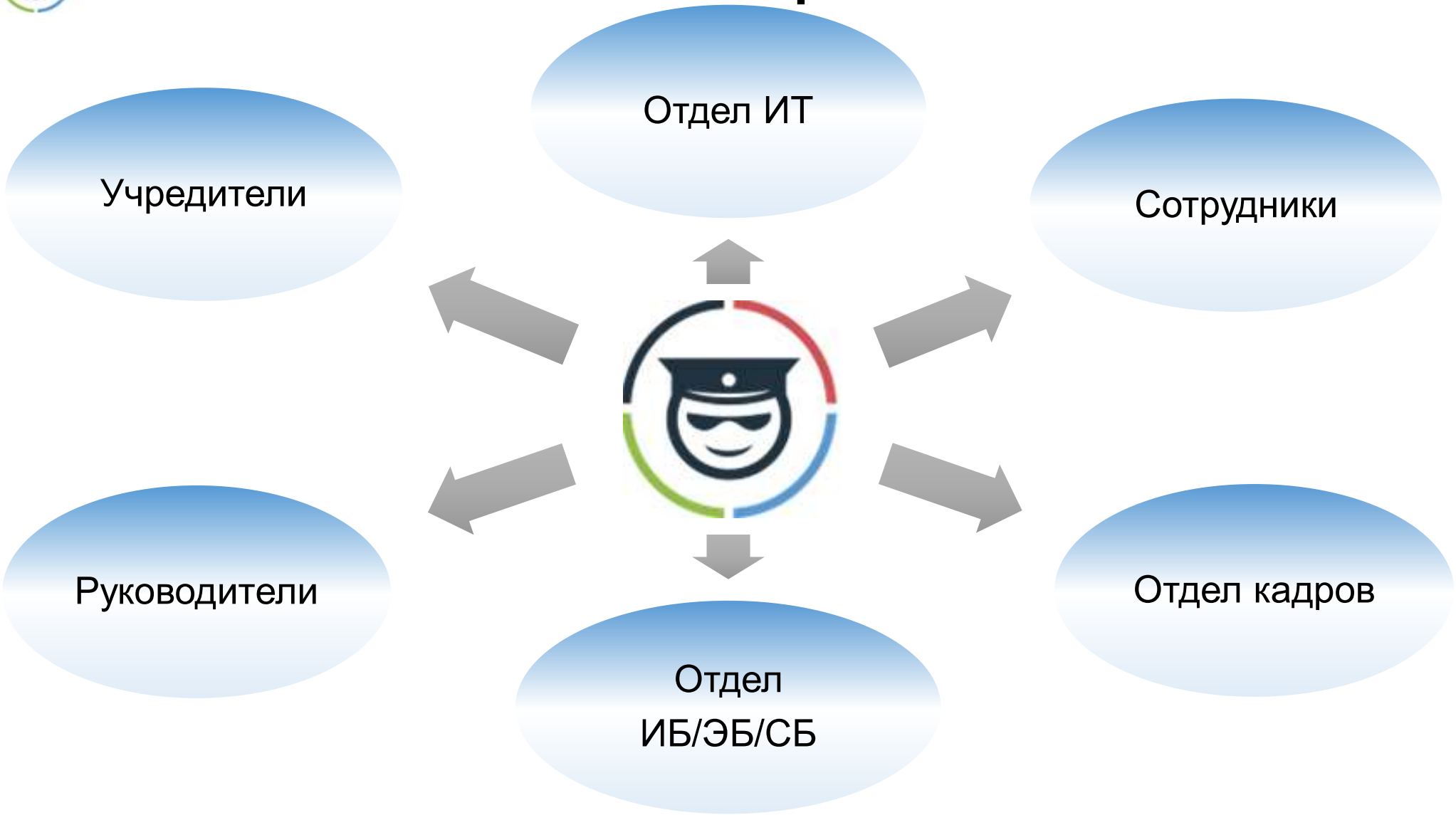
Статус	Компьютер	Поставщик
В наличии	DESKTOP-N36I35U	TeamViewer

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

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



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

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

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