



**Обеспечение информационной безопасности
посредством контроля информационных потоков
цифрового предприятия**

Чеплиёв Максим

Специалист отдела аналитики

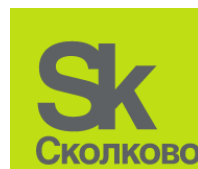
ООО Атом Безопасность

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





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

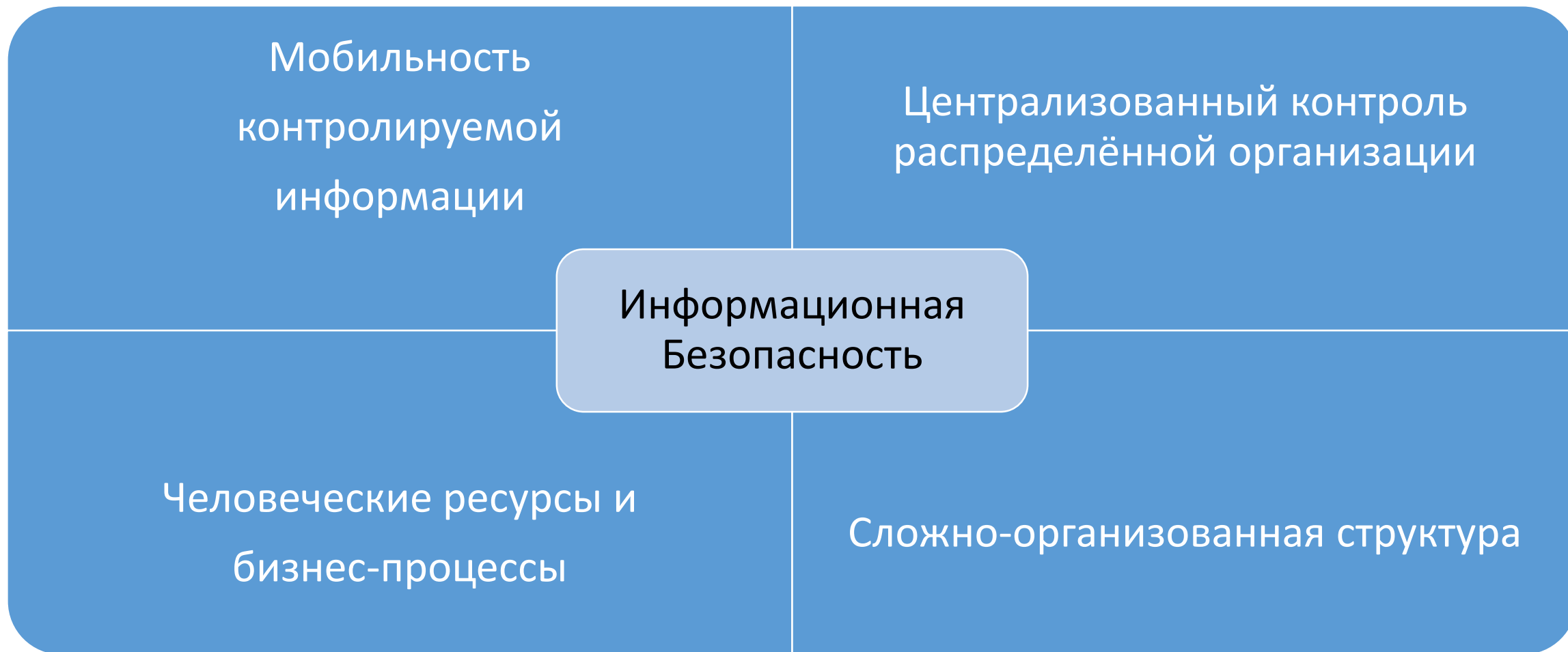


Учет рабочего времени и оценка продуктивности сотрудников
Мониторинг бизнес-процессов и анализ эффективности сотрудников



Инвентаризация программного и аппаратного обеспечения
Удаленное администрирование машин пользователей

Особенности обеспечения безопасности цифрового предприятия.



Организация системы контроля



Законы

- **№149 ФЗ «Об информации, информационных технологиях и о защите информации».**
- **№98 ФЗ «О коммерческой тайне».**
- **№152 ФЗ «О защите персональных данных».**

Ваши действия

- Определить и довести до работников правила использования средств хранения, обработки и передачи информации .
- Разработать и довести до работников регламент проведения мониторинга.
- Получить согласие работников на проведение мониторинга использования им средств хранения, обработки и передачи информации.
- Включить положения об обязательстве работника соблюдать правила использования средств коммуникации и согласие на мониторинг в трудовой договор (дополнительное соглашение к трудовому договору).



ФСТЭК России
Федеральная служба
по техническому и
экспортному контролю

приказ ведомства №35 от 20.02.2020
об обеспечении безопасности КИИ

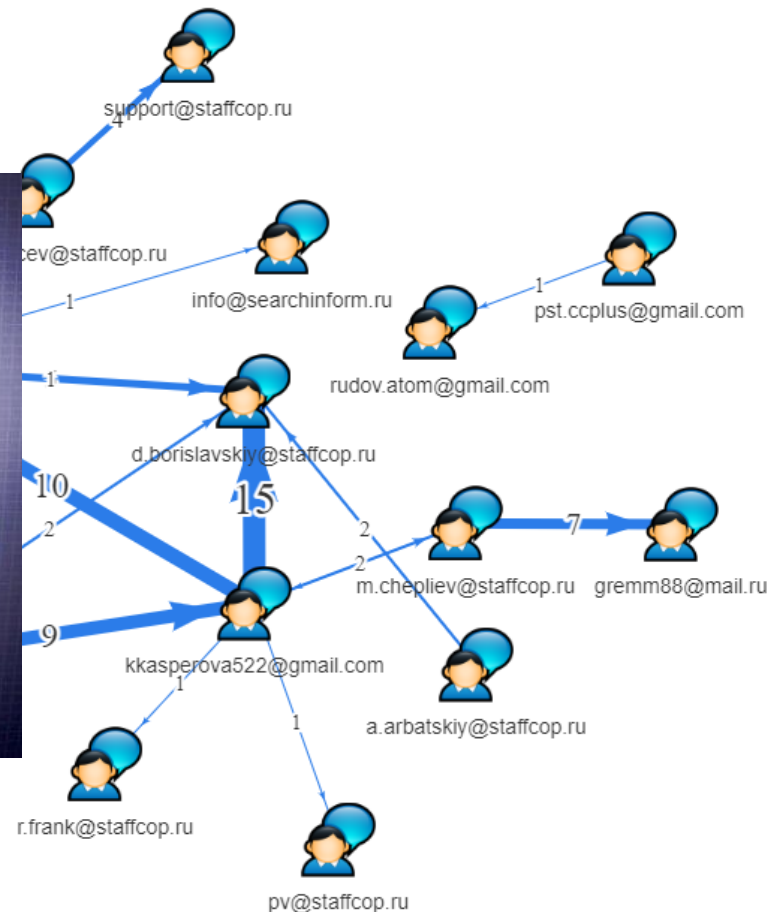


Банк России

ГОСТ Р 57580.1-2017

Безопасность финансовых (банковских) операций.

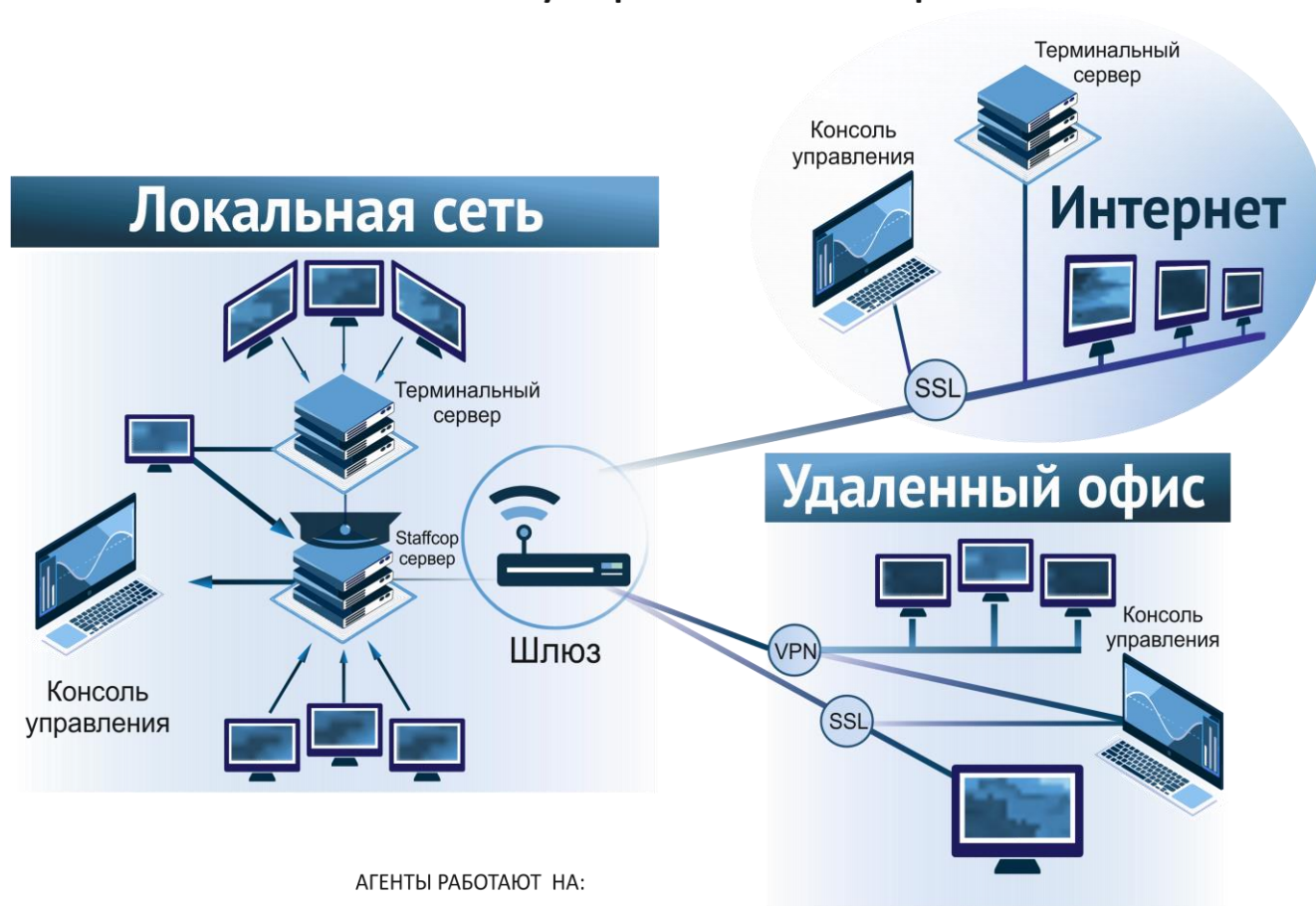
- Какое дополнительное ПО, База данных или ОС требуются для внедрения
- Насколько трудозатратно развертывание системы?.
- Система не должна мешать организации полноценно функционировать.
- Весь ли функционал вам необходим? Возможно ли использование более дешевой системы закрывающей ваши задачи?
- ФСТЭК? Другие законодательные аспекты внедрения.
- Возможность использования возможностей системы другими отделами.
- Система должна решать задачи поставленные бизнесом.





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

- Электронная почта
- Съемные 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

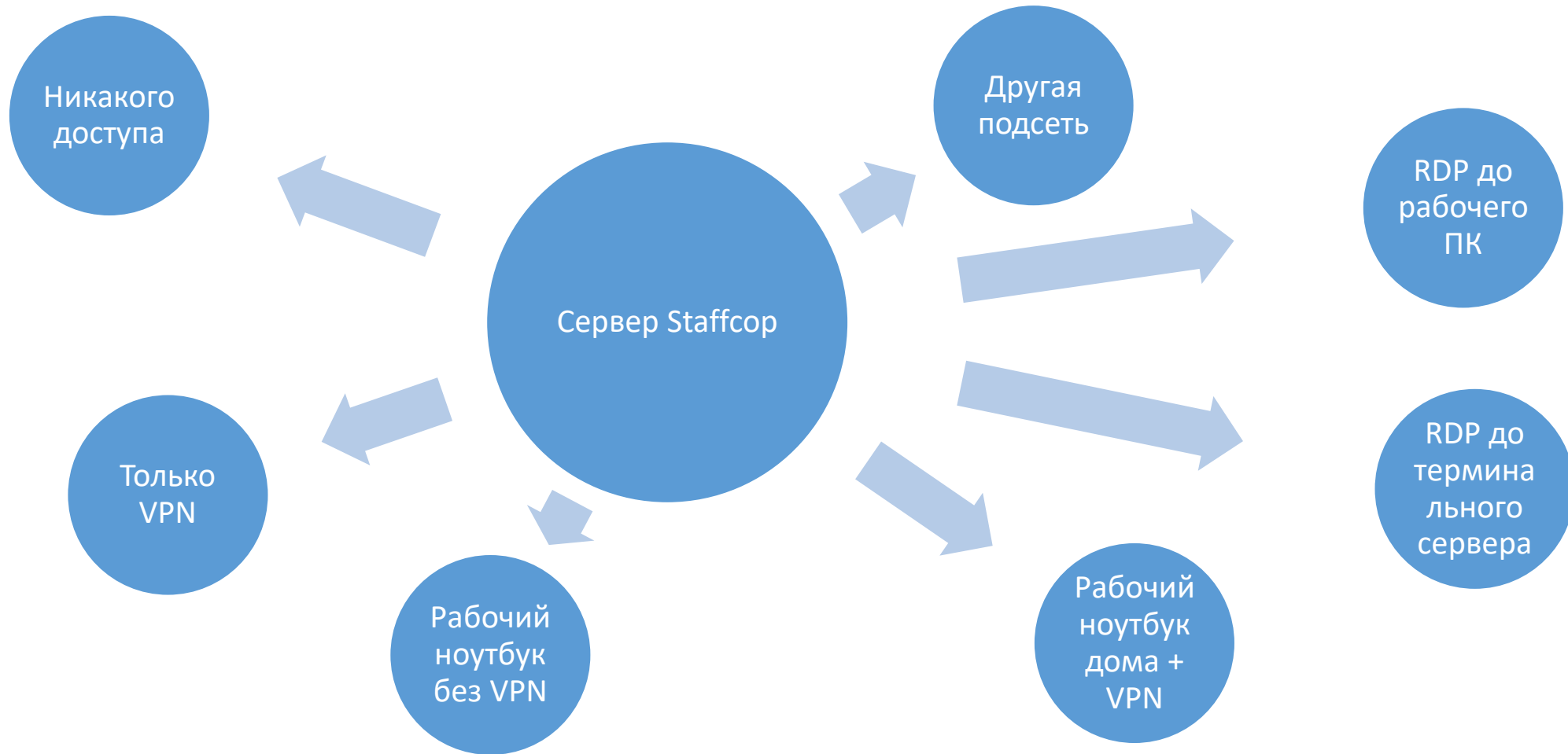
Почтовые протоколы

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

Декодирование
сервисов веб-почты и
соц.сетей

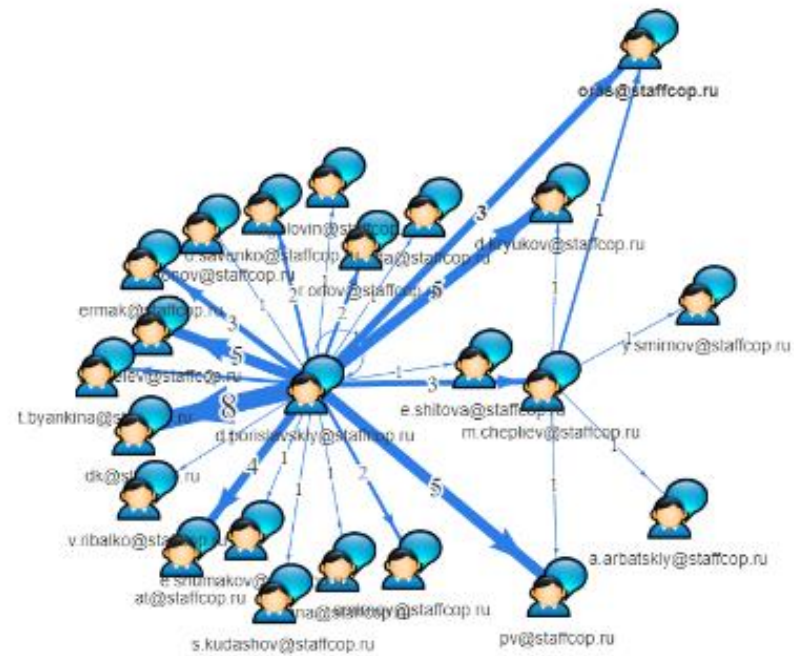
- Mail.ru, Yandex.ru, gmail.com и т.п.
- VK, FB, Одноклассники и т.п.

Контроль разветвленной сети и удаленных сотрудников.



- 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







Организация расследований ИНЦИДЕНТОВ

Инциденты

Статусы

Группы инцидентов

Шаблоны реагирования

Сводные отчеты

Недоменная отправка файлов

Отправка на флешку

Фильтр 1

Переписка: Отправитель

kkasperova522@gmail.com

arseniieset@ngs.ru

Пользователь: Полное имя

Устройство: ID устройства

Нет данных за период, попадающих под фильтр

39

Конфиденциальная информация (18.7%)

27

Пароль в браузере (12.9%)

20

Развлекательные ресурсы (9.6%)

18

Торговые площадки и доски объявлений (8.6%)

В основной интерфейс Инциденты

Фильтр

Новый инцидент

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 недозволненной информации		Admin User				

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

www.staffcop.ru



www.staffcop.ru



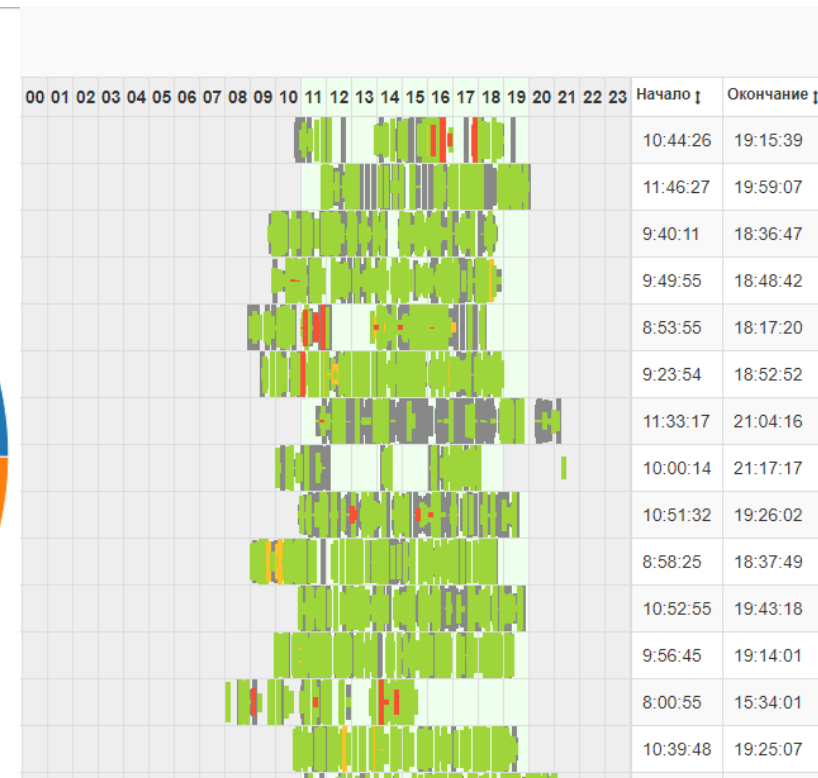
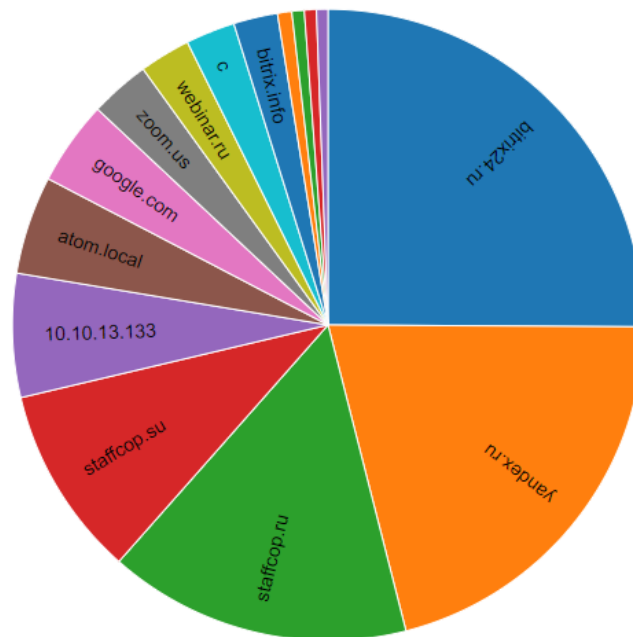
Отчёт отражает суммарное продуктивное/непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя

■ Продуктивное время ■ Непродуктивное время ■ Нейтральное время

www.staffcop.ru

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	crocodile.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

Ограничение доступа и передачи информации

Метки и блокировка доступа

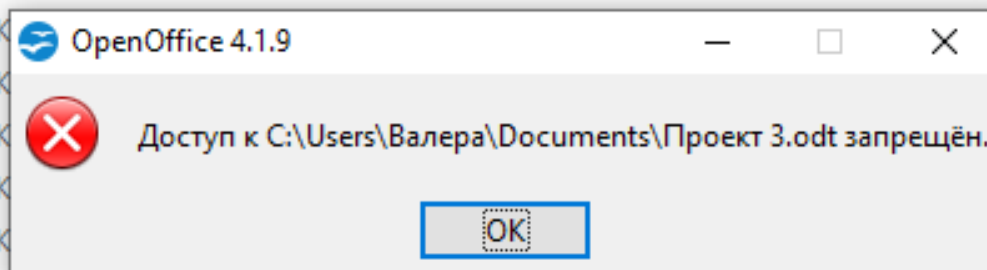
Справка

☒ 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:			
Имя пользователя	equals	Ксения	Удалить правило 
And			
Контент	matches	договор x 1234561234 x ИНН x	And
And			
Имя приложения	equals	outlook.exe	
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 приложений, сайтов и 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

☒ USB устройства Контроль подключений и отключений USB-устройств. Перехват файловой активности. Файловая активность и Теневое копирование".

☐ Блокировать USB накопители Блокировка всех USB-накопителей. Перекрывает правила мониторинга "Блокировка USB" и "Блокировка - USB-класс". Требуется включение модуля "USB устройства"

☒ USB накопители только для чтения Переводит все USB-накопители в режим "Только чтение". Требуется 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

+

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/ui/

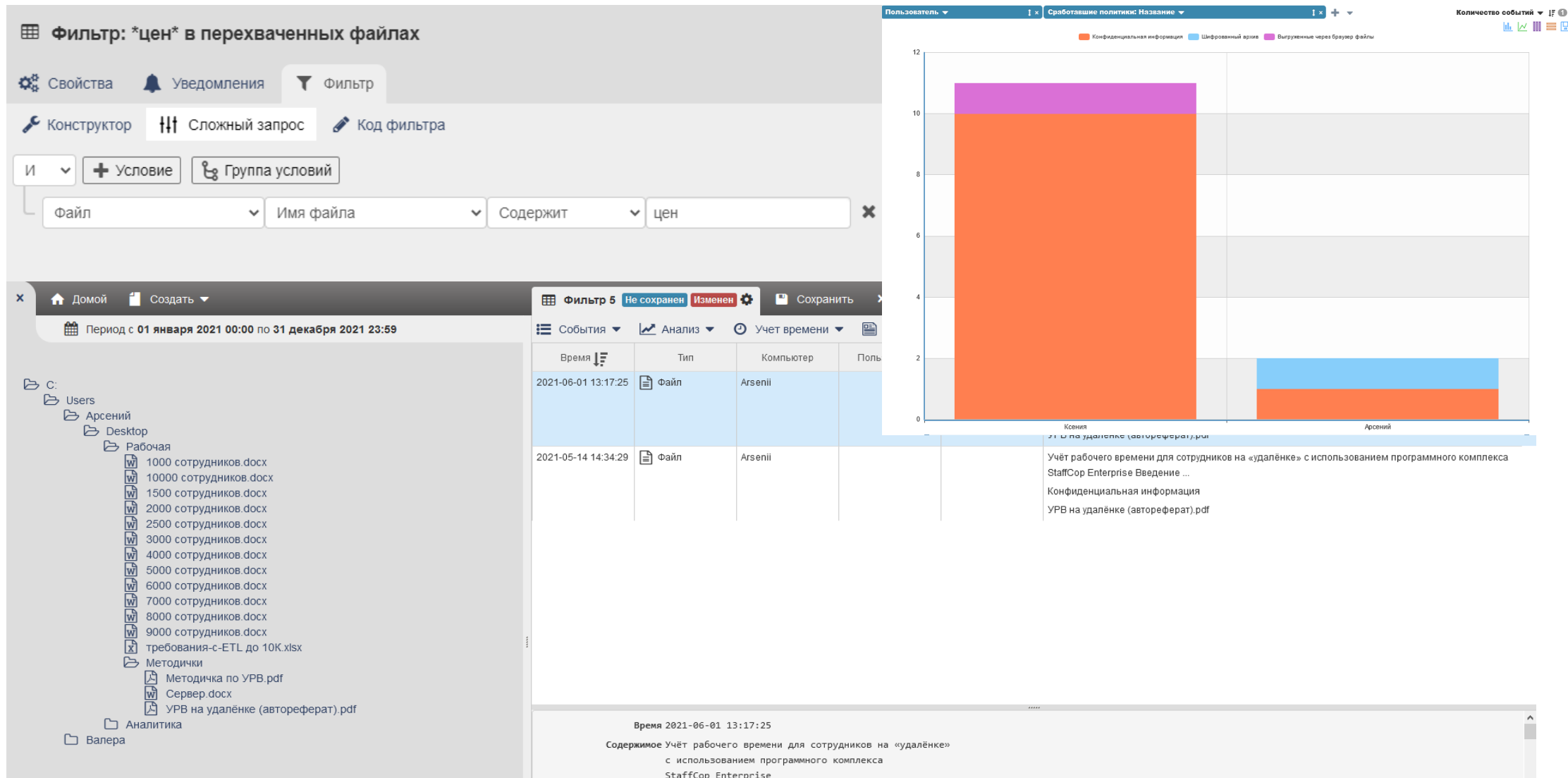
x

Разрешить

+

USB\VID_090C&PID_1000\0113000000000602

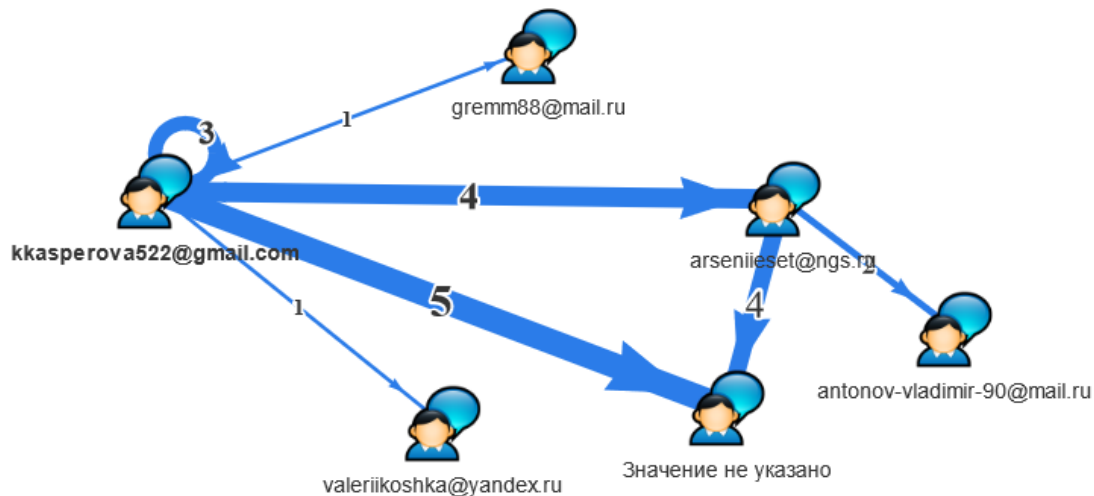
x



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 RE: Проверка связи.html ↓	5.2 Kb	Mail ➡
				Maxim_Chepliev_79232470277	Скачать RE: Проверка связи.html ↓	4.2 Kb	Mail ➡
				kkasperova522@gmail.com	Скачать RE: Проверка связи.html ↓	184 B	Mail ➡
				arseniieset@ngs.ru	Скачать Fwd: сохранить.html ↓	1.6 Kb	Mail ➡
				-90@mail.ru	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 ➡

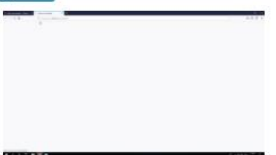


Паспортные данные и кредитные карты

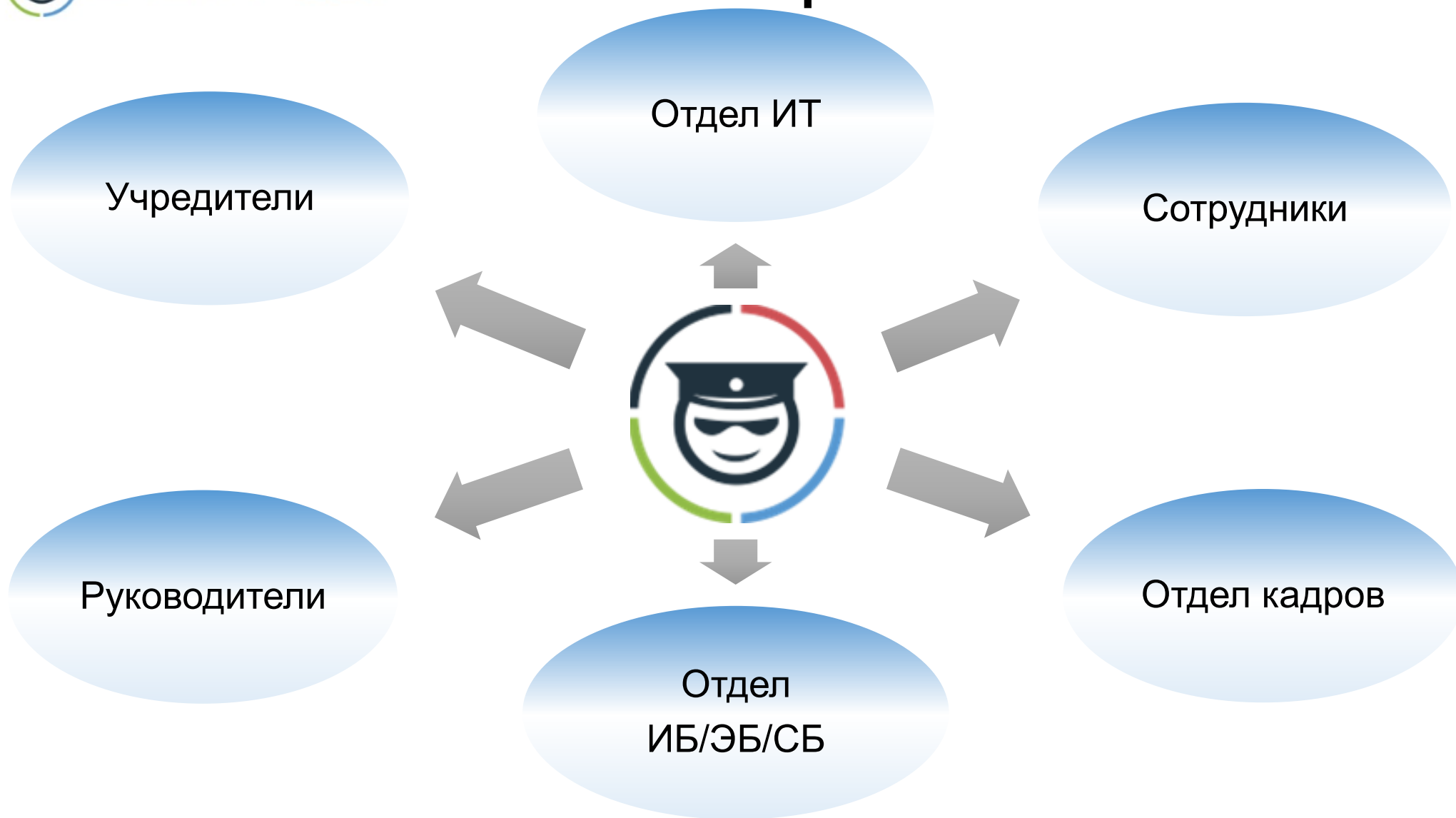


DemoZoneVM2	Ксения	 chrome.exe	Скачать Documents.7z ↓ Кредитные карты Ксения Касперова Сначала деньги, потом остальное 4276160971368577 сбер вс, 14 июн. 2020 г. в 16:06, Даниил Бориславский <d.borislavskiy@staffcop.ru>: норм, давай ещё вс, 14 июн. 2020 г. в 16:01, Ксения Касперова <kkasperova522@gmail.com>: Как договаривались.
-------------	--------	--	--

Доски объявлений и продажа списанного оборудования.

Пользователь: Полное имя Сайт Приложение: Заголовок окна				События Анализ Учет времени Отчеты			
			Количество со				
Арсений Есетовский	avito.ru	cisco asa - Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	6				
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 Juniper srx100 купить в Кемерово с доставкой Бытовая электроника Авито - Mozilla Firefox	2	08.07.2020 12:47:31	08.07.2020 12:47:18	08.07.2020 12:47:12	08.07.2020 12:47:04
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнауле с доставкой Бытовая электроника Авито - Mozilla Firefox	2				
Арсений Есетовский	avito.ru	Cisco asa 5505 купить в Новосибирске с доставкой Бытовая электроника Авито - Mozilla Firefox	2	08.07.2020 12:46:49	08.07.2020 12:46:37	08.07.2020 12:46:15	08.07.2020 12:46:06
Арсений Есетовский	avito.ru	Cisco ASA 5505 купить в Новосибирске с доставкой Бытовая электроника Авито - Mozilla Firefox	2				
Арсений Есетовский	avito.ru	Сетевой экран Cisco ASA5505 купить в Новосибирске с доставкой Бытовая электроника Авито - Mozilla Firefox	2	08.07.2020 12:45:49	08.07.2020 12:45:22	08.07.2020 12:45:07	
Арсений Есетовский	avito.ru	Межсетевой экран Cisco ASA 5510 купить в Новосибирске с доставкой Бытовая электроника Авито - Mozilla Firefox	2				
Арсений Есетовский	avito.ru	Продам Cisco ASA5510-SEC-BUN-K9, WS-C2960PD-8TT-I купить в Новосибирске Бытовая электроника Авито - Mozilla Firefox	2				
Арсений Есетовский	avito.ru	Авито — объявления в Новосибирске — Объявления на сайте Авито - Mozilla Firefox	2				
Арсений Есетовский	avito.ru	Cisco asa5505 купить в Барнауле с доставкой Бытовая электроника Авито	1				
Арсений Есетовский	avito.ru	Cisco 2821 ASA5510 Cisco 1760 Juniper srx100 купить в Кемерово с доставкой Бытовая электроника Авито	1				
Всего: 11, Количество							

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



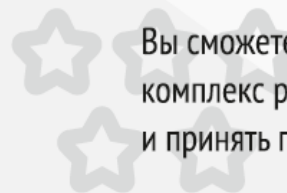
Развертывание пилотного проекта обычно занимает не более одного дня

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