



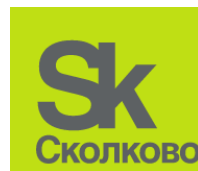
**Контроль информационных потоков – комплексное
обеспечение информационной безопасности
инфраструктуры организации.**

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

Организуемся

Что?

Информация

Где хранится?

Как используется?

Как передается?

Чем?

ПО

Люди

Как?

Своевременное реагирование

Шаблонное реагирование

Итог

Без подготовки – никак.

ПО

Должно отвечать поставленным задачам.

Стоимость ПО не должна превышать стоимость утечки.

Внедрение и настройка.

Люди

Подготовка и обучение.

Организация.

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.

Что и как мы контролируем.

Информация

- Доступ
- «Цена»
- Работа
- Перемещение

Каналы

- Надежность
- «Контроль»
- «Регламент»

Люди

- Доступ к информации
- Работа с информацией
- Передача информации

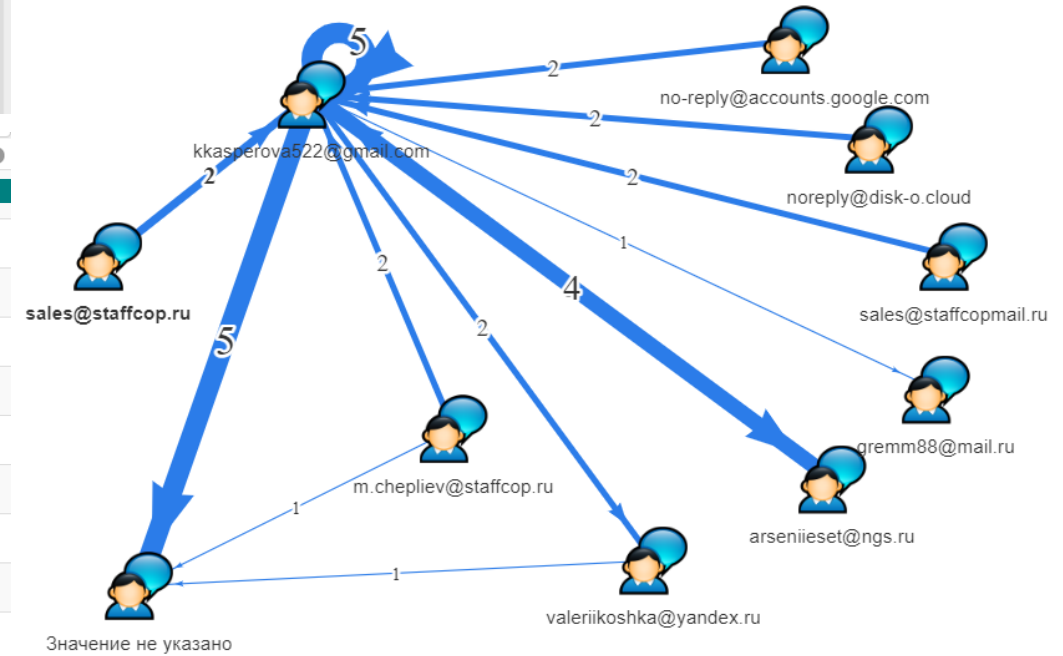
Инциденты

- «Точность»
- «Оперативность»
- «Организованность»

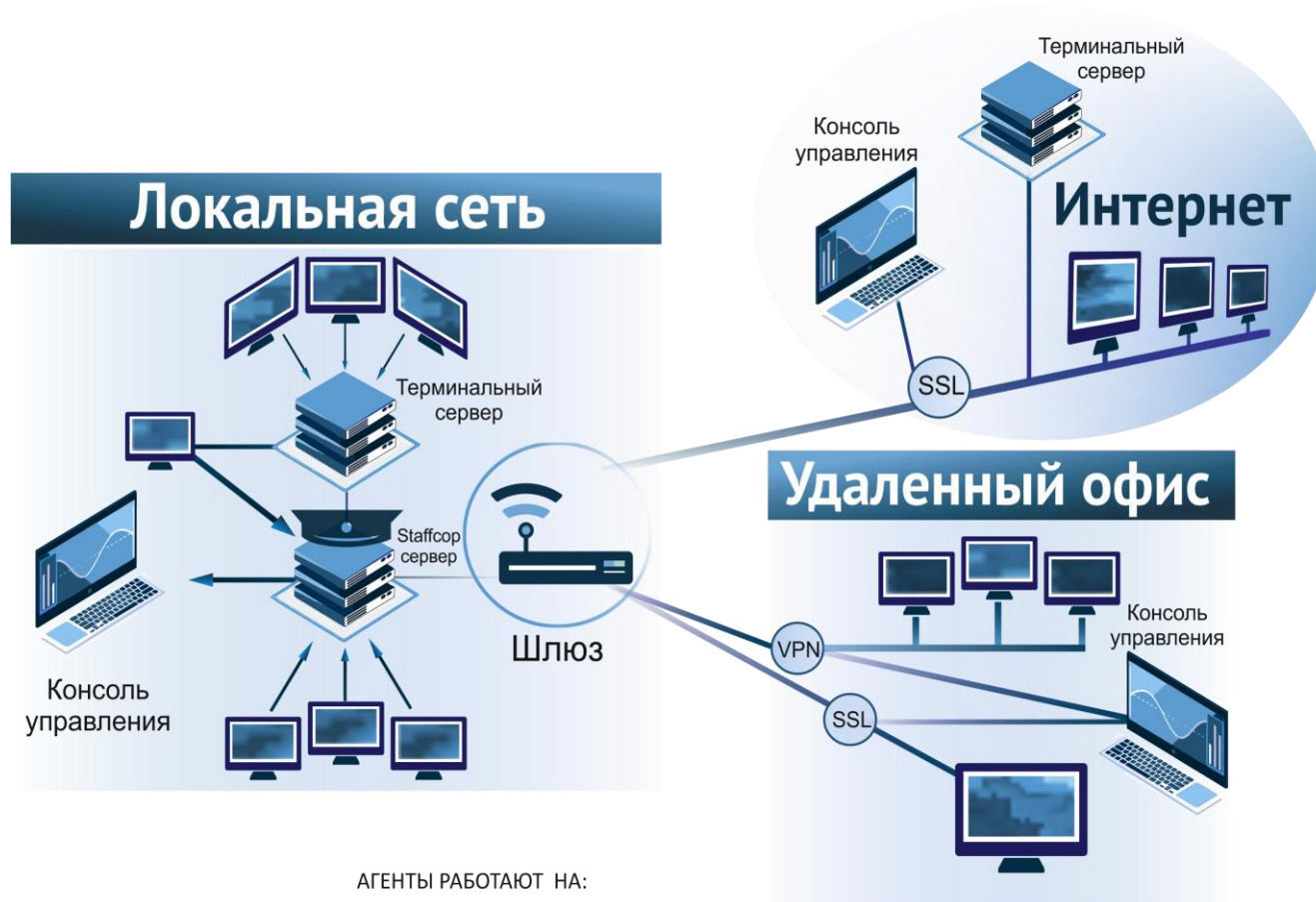
С:

- Users
 - Арсений
 - Валера
 - Downloads
 - Тест договор.backup.xlsx
 - Staffcop Enterprise - Дашборд по сотруднику за выбранный период.pdf
 - Staffcop Enterprise - переписка сотрудника (осуждает руководителя).pdf
 - Staffcop Enterprise - пример другого отчёта по рабочему времени.pdf
 - Staffcop Enterprise - пример отчёта по инцидентам информационной

Пользователь	Переписка: Канал общения	Файл: Имя файла	Количество событий
Ксения	Skype	Тест договор.backup.xlsx	3
Ксения	Mail	RE: Проверка связи.html	2
Ксения	Mail	Пресс-релиз 4.8.docx	1
Ксения	Mail	Тестовое сообщение Microsoft Outlook.html	1
Ксения	Mail	Цены.docx	1
Ксения	Telegram	image_2021-05-14_14-22-19.jpg	1
Ксения	Telegram	TC8br_oRTMKMi_sgJfAPsg.png	1
Ксения	Mail	500.jpg	1
Ксения	Telegram	Отчёт12.7z	1
Ксения	Mail	staffc.html	1



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

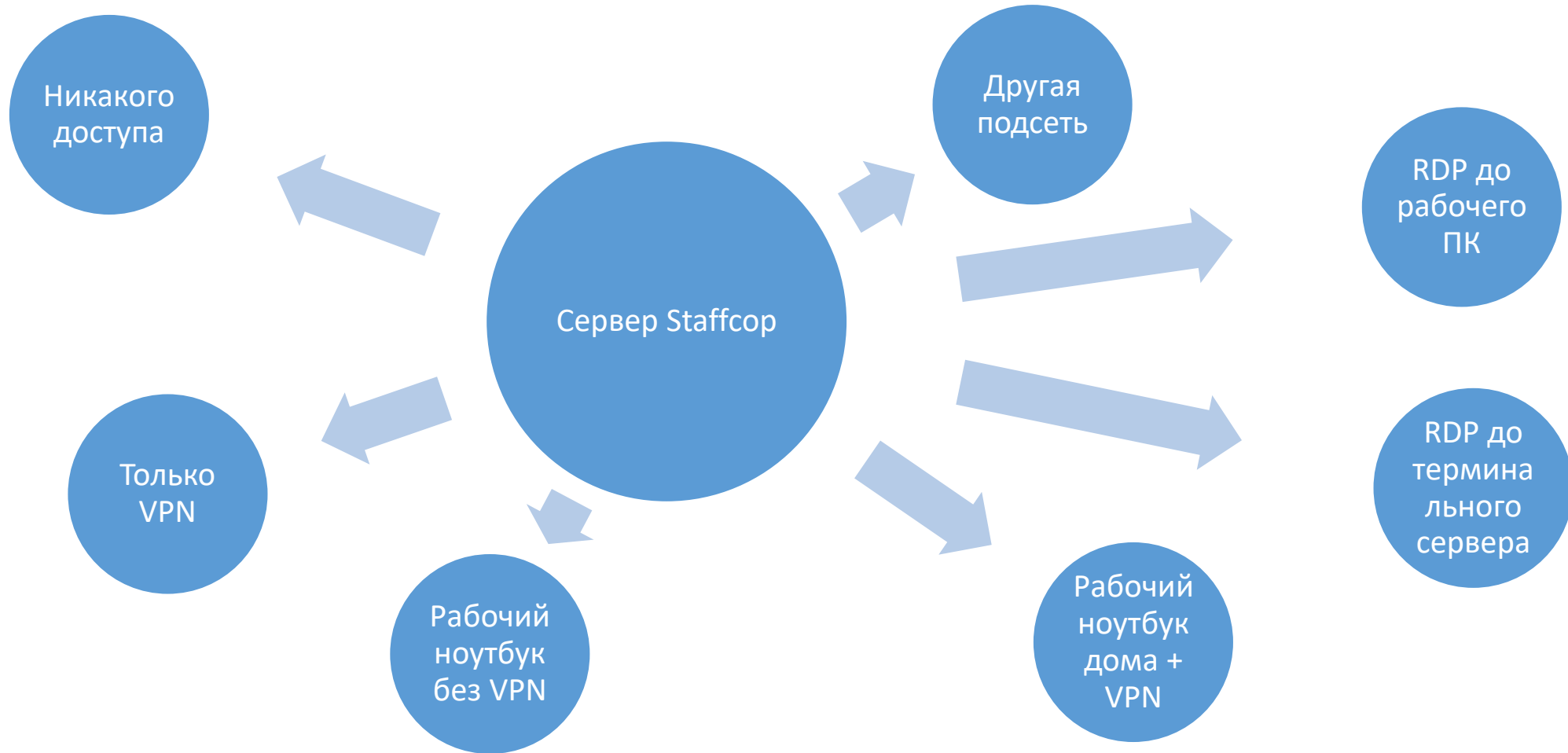
Почтовые протоколы

- 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 разветвленной сети и удаленных сотрудников.



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

Фильтр: Фильтр 4

Свойства Уведомления Фильтр

Активировать уведомления

Регулярность

- Новые
- Ежедневно
- Еженедельно
- Ежемесячно 1 числа

Время отправки 06:00

- Лента событий Шаблон
- HTML
- PDF
- Разделить по пользователям
- Отправлять только если есть данные
- Отправить по почте
- Сохранить отчет на диск


Создать инцидент

Шаблон реагирования Наказать

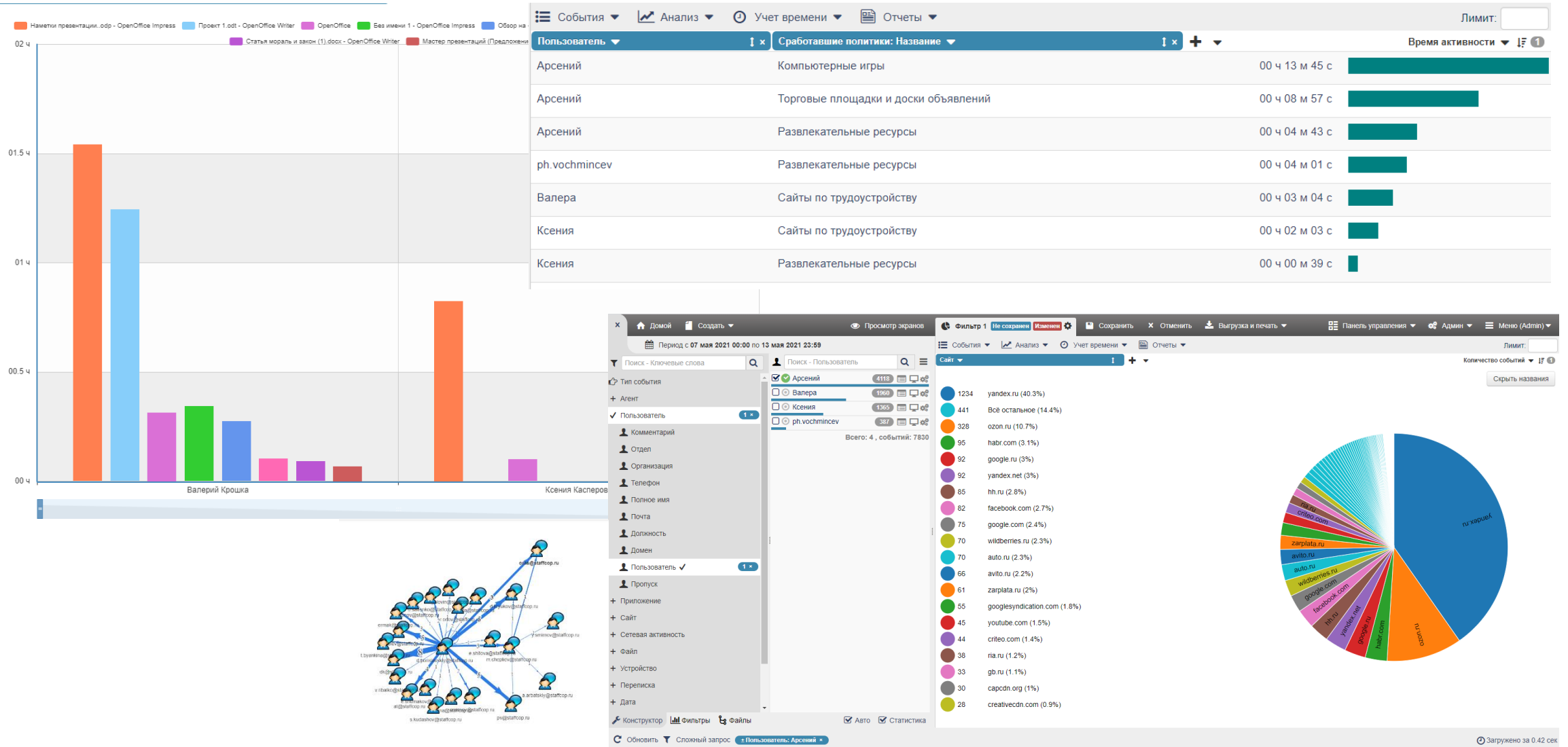
Группа инцидента Default group

Кому admin(admin@example.com)

Адреса Поиск адресов...



Анализ собранной информации



Наличие информации

Домой Создать

Период с 04 мая 2021 00:00 по 02 июня 2021 23:59

Поиск - Ключевые слова

Поиск - Агент: Компьютер

Тип события 1 x

Агент

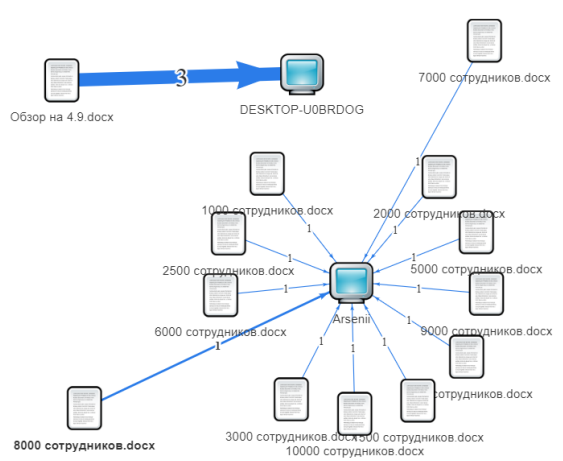
IP адрес

Группа

Сотрудник

Компьютер ✓

Всего: 2, событий: 166



Активация Windows
Чтобы активировать Windows, перейдите в раздел "Параметры".

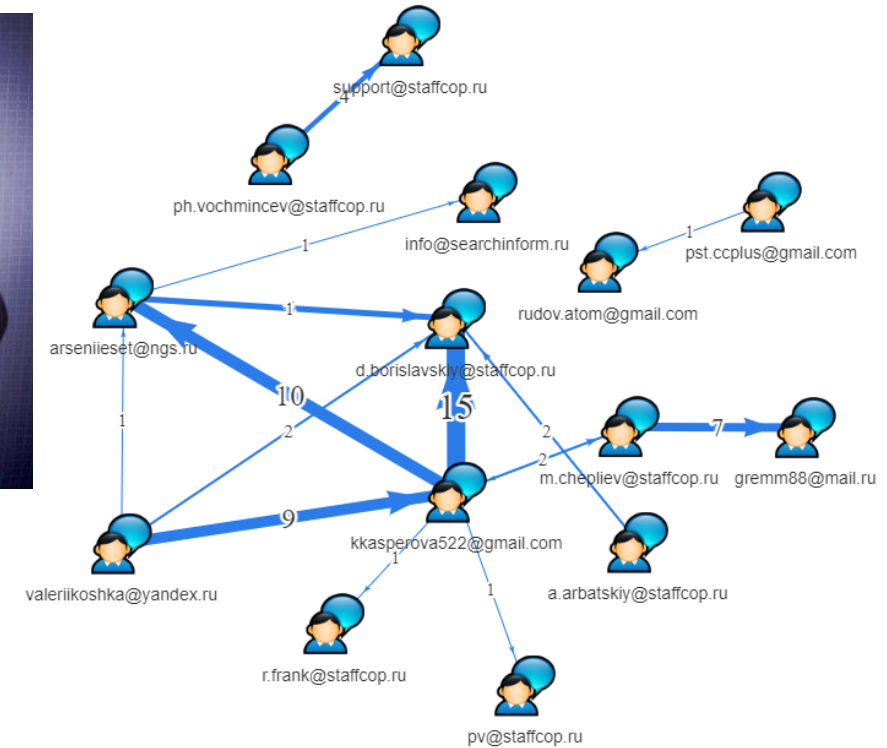
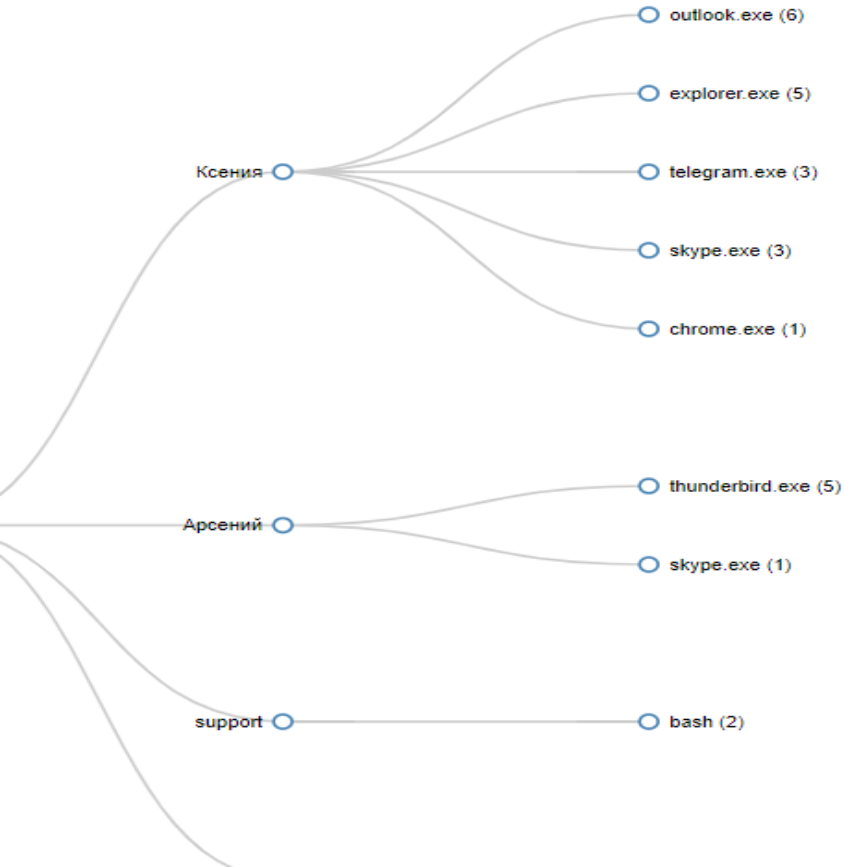
Фильтр 4 Не сохранен Изменен

События Анализ Учет времени Отчеты

Лимит:

Файл: Имя файла	Файл: Путь	Агент: Компьютер	Количество событий
Документ Microsoft Word.docx	C:\Users\Валера\Desktop\Документ Microsoft Word.docx	DESKTOP-U0BRDOG	4
Тест договор.backup.xlsx	C:\Users\Валера\Downloads\Тест договор.backup.xlsx	DESKTOP-U0BRDOG	4
цены на всё.docx	C:\Users\Валера\Downloads\цены на всё.docx	DESKTOP-U0BRDOG	3
1.pdf	C:\Users\Валера\Documents\1.pdf	DESKTOP-U0BRDOG	3
Наметки презентации..odp	C:\Users\Валера\Documents\Наметки презентации..odp	DESKTOP-U0BRDOG	3
Обзор на 4.9.docx	C:\Users\Валера\Downloads\Обзор на 4.9.docx	DESKTOP-U0BRDOG	3
Отчёт12.docx	C:\Users\Валера\Documents\Отчёт12.docx	DESKTOP-U0BRDOG	3
Отчёт12.docx	C:\Users\Валера\Downloads\Отчёт12.docx	DESKTOP-U0BRDOG	3
Отчёт13.docx	C:\Users\Валера\Documents\Отчёт13.docx	DESKTOP-U0BRDOG	3
помятка для презентации.odt	C:\Users\Валера\Documents\помятка для презентации.odt	DESKTOP-U0BRDOG	3

Каналы утечки и взаимосвязи



Агент: Компьютер	Пользователь	Устройство: ID устройства	Количество событий
DESKTOP-N36I35U	Ксения	USB\VID_090C&PID_1000\0113000000000602	5

- 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



Две руки, два глаза, один мозг.

В основной интерфейс
Инциденты
Фильтр
+ Новый инцидент

	ID ↓	Дата	Тема	Группа	Статус	Создал	Назначен	Приоритет	Шаблон реагирования	Фильтр
Инциденты	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
Статусы	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
Группы инцидентов	11	26.05.2021 12:59	На основании фильтра 1005 "Фильтр 1"	Утечка данных		Admin User	Maxim Chepliev	Незначительный	Ограничить доступ к данным и каналам передачи данных	Фильтр 1
Шаблоны реагирования									Ограничить доступ к	
Сводные отчеты										

Недоменная отправка файлов

Переписка: Отправитель ↓

kkasperova522@gmail.com	5	<div style="width: 100%; height: 10px; background-color: #008080;"></div>
arseniieset@ngs.ru	4	<div style="width: 100%; height: 10px; background-color: #008080;"></div>


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

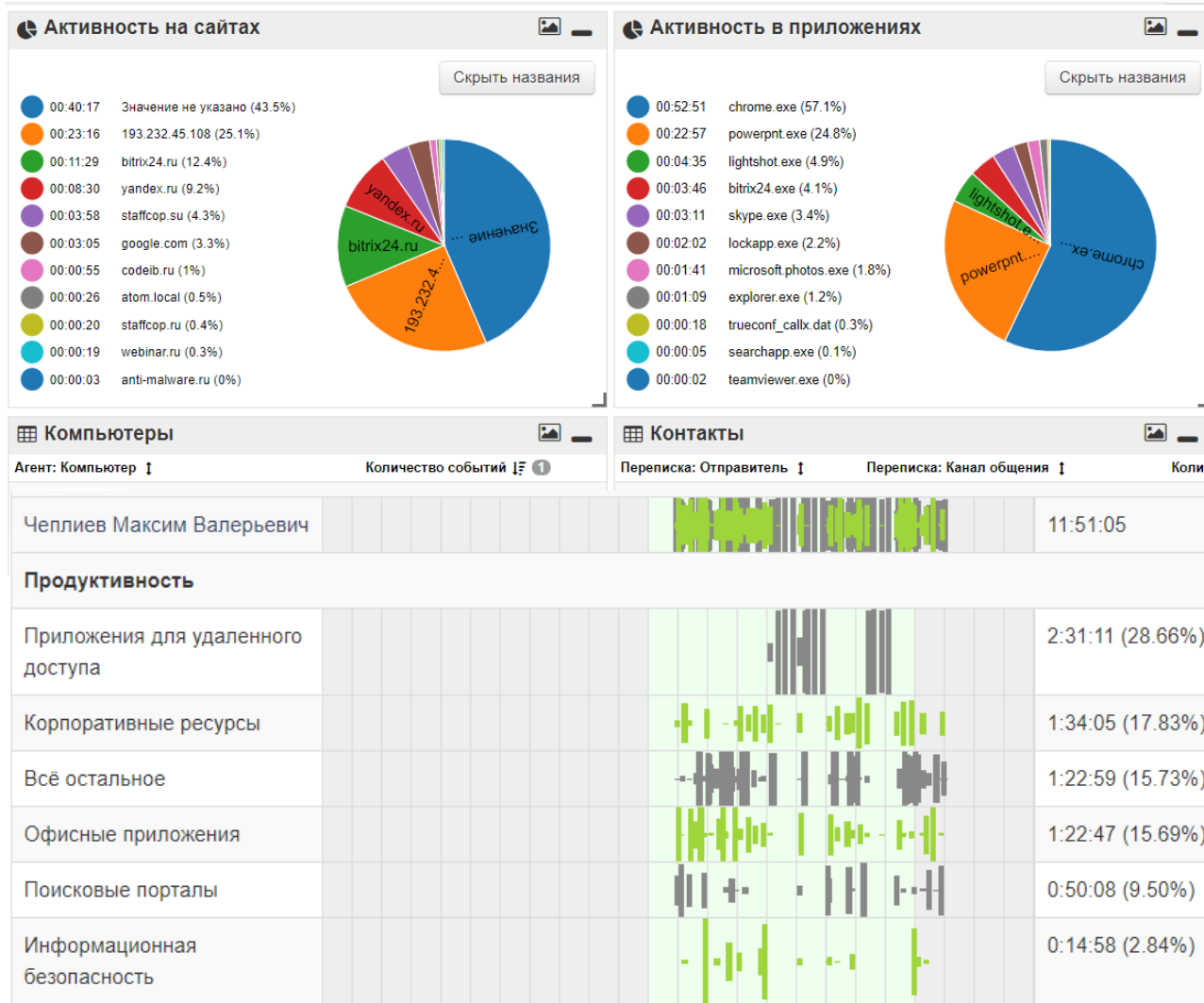
Время отправки:

Создать инцидент

Шаблон реагирования:

Группа инцидента:

Кому:



- 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

Мониторинг

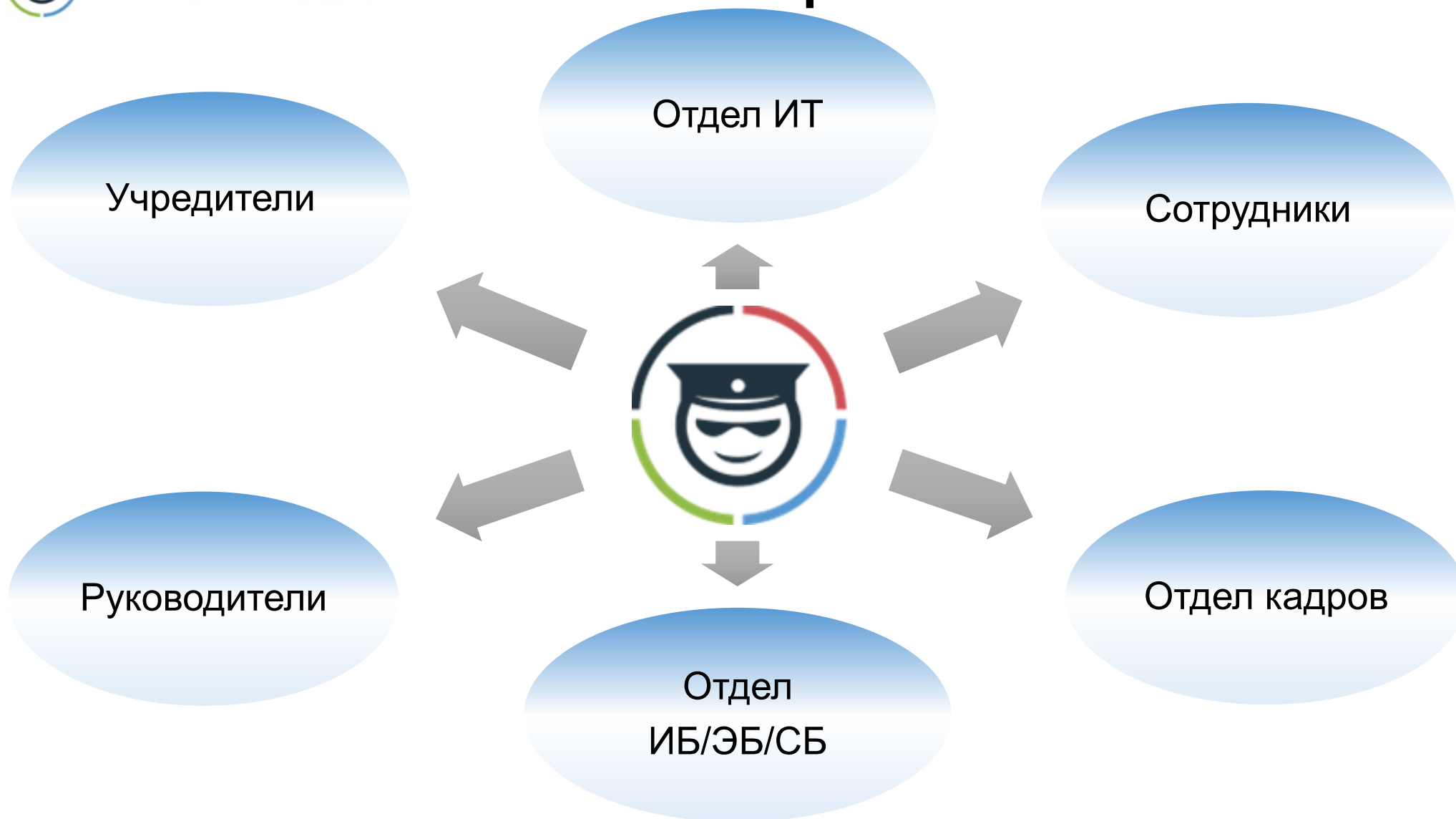
Блокировки

Инвентаризация ПО и «железа»

Уровни доступа к данным и функционалу в системе

Интеграция с SIEM

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



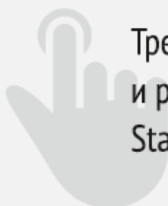
Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро



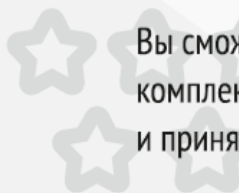
Развертывание пилотного проекта обычно занимает не более одного дня

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