



Контроль над информационными потоками и действиями сотрудников на удалёнке и в офисе.

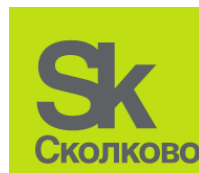


Даниил Бориславский
Руководитель аналитического
отдела
ООО Атом Безопасность
db@staffcop.ru





- 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.



академпарк

Технопарк Новосибирского Академгородка



BIS SUMMIT
2018



ФСТЭК России

Федеральная служба
по техническому и
экспортному контролю



Минкомсвязь
России

Тут могли быть слайды с числами,
графиками, статистикой и даже
картинками, но...



Зачем нужен контроль над инф. потоками?



Cisco Маршрутизатор /свич /коммутатор / межсетевой 1 500 Р

Добавить в избранное Добавить заметку Вчера в 11:25



Купить с доставкой

Доставка в пункт выдачи
Гарантия возврата денег, если товар не подойдет. Как это работает

Показать телефон

Написать сообщение

Отвечает около 30 минут

5.0 8 отзывов

52 объявления пользователя



ФСТЭК России

Федеральная служба по техническому и экспортному контролю



Банк России

приказ ведомства №35 от 20.02.2020
об обеспечении безопасности КИИ

ГОСТ Р 57580.1-2017

Безопасность финансовых (банковских) операций.



Комплексное решение по информационной безопасности, учёту рабочего времени и контролю эффективности сотрудников



учет рабочего
времени



эффективность
персонала



информационная
безопасность

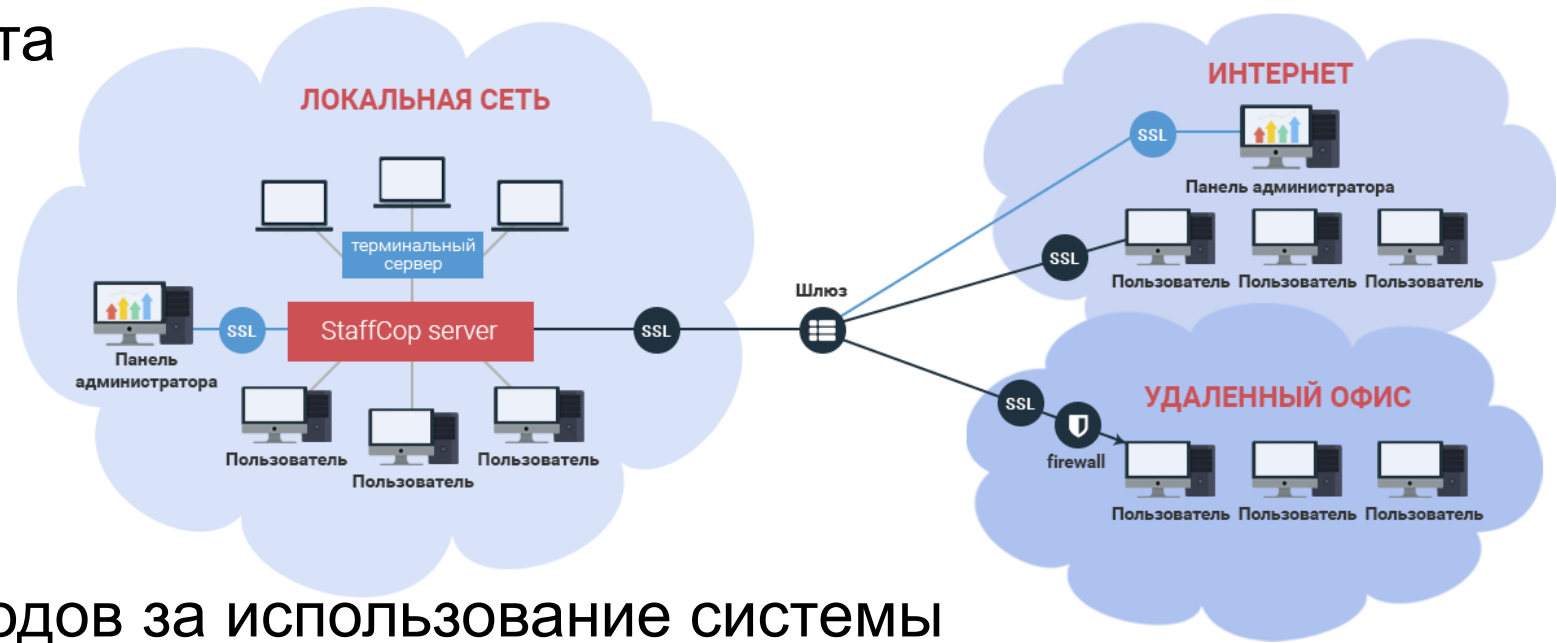


расследование
инцидентов



удаленное
администрирование

- Для работы сервера уже достаточно всего одной виртуальной машины
- Контроль ПК под управлением OS Windows, Linux, MacOS
- Система готова к сбору данных сразу после установки
- Удалённая установка агента
- OS Linux, BD PostgreSQL



- Нет дополнительных расходов за использование системы



Декодирование сервисов веб-почты и социальных сетей:

- mail.ru, yandex.ru, gmail.com...
- VK, FB, Одноклассники, LinkedIn...

Почтовые протоколы:

- SMTP / SMTPs
- IMAP
- POP3 / POP3s
- MS Exchange

Передача гипертекстовой информации и файлов:

- HTTP / HTTPs
- FTP / FTPs

Интернет-мессенджеры

- Skype
- ICQ, QIP, Jabber (XMPP)
- Mail.ru Agent
- Yahoo и другие

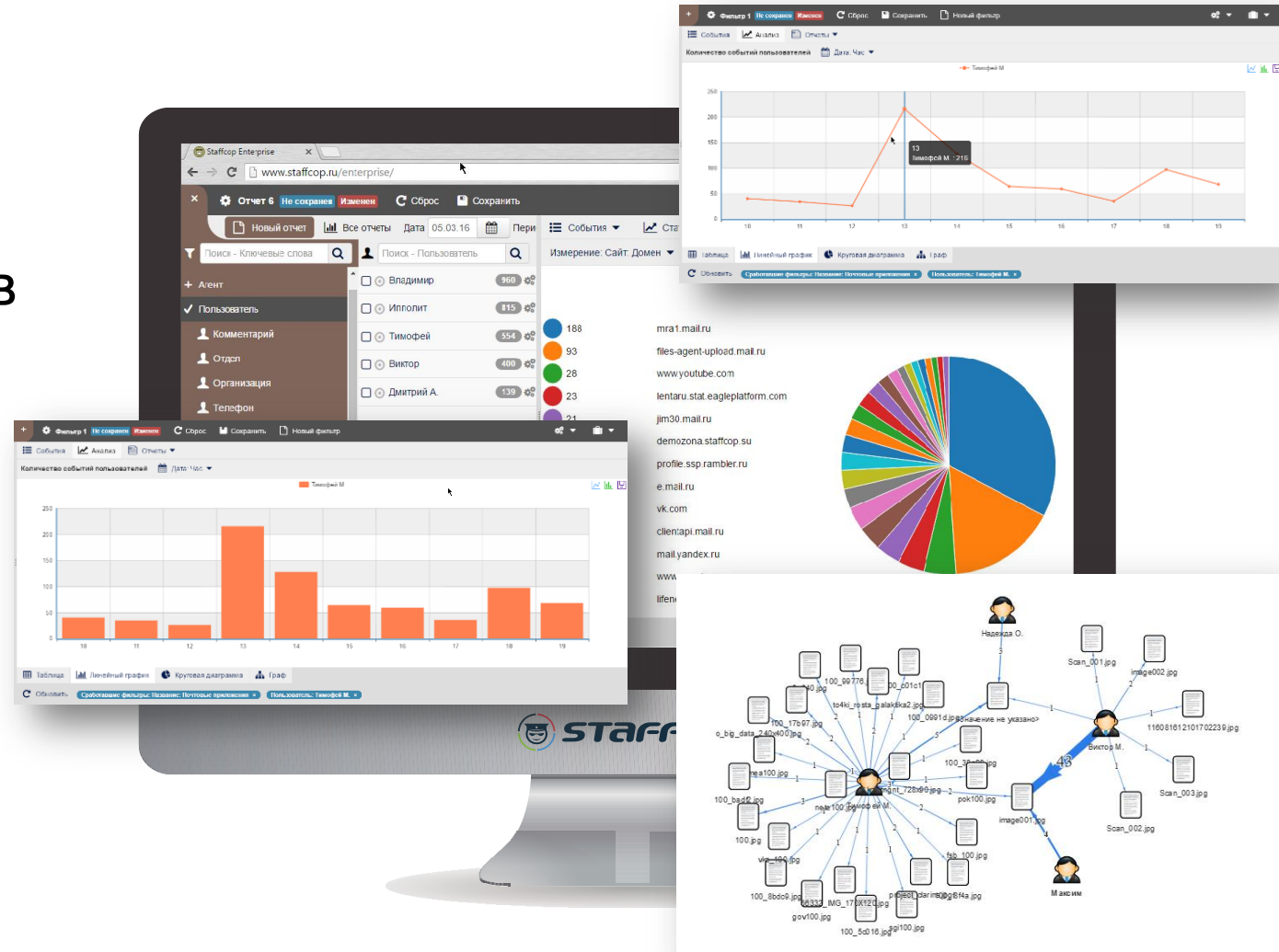
USB-порты

- контроль и блокировка

Теневое копирование файлов

- из электронной почты
- со съемных носителей
- переданных через интернет
- отправленных на печать

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





- Мониторинг
- Блокировки
- Инвентаризация ПО и «железа»
- Интеграция с SIEM
- Разные доступы для разных пользователей системы



Картинки о том
как всё будет
работать



Скриншоты
и примеры
как работает




Учёт рабочего времени и его оценка

00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Начало ↓	Окончание ↓	Общее время ↓	Активное ↓	Простой ↓
																								9:54:29	21:15:32	11:21:03	6:14:19	5:06:44
																								9:07:06	18:22:55	9:15:49	8:34:07	0:41:42
																								11:20:35	20:01:01	8:40:26	7:04:36	1:35:50
																								17:23:27	20:57:18	3:33:51	1:41:48	1:52:03
																								12:53:25	21:14:43	8:21:18	3:46:49	4:34:29
																								10:35:44	19:10:12	8:34:28	7:17:27	1:17:01
																								0:10:40	22:15:10	22:04:30	10:35:12	11:29:18
																								0:00:33	23:54:10	23:53:37	12:44:53	11:08:44
																								10:51:19	19:52:45	9:01:26	8:11:35	0:49:51
																								11:05:09	23:19:51	12:14:42	9:13:23	3:01:19

Дисциплина

Активность

Продуктивность

Время ↓	Компьютер	Пользователь	Приложение	Контент	Связано с	Страниц	Размер	Получатели
2020-07-08 12:34	DemoZoneVM2	Ксения	 explorer.exe	Скачать Входные цены.xlsx ↓	FileOperation →		8.2 Kb	
2020-06-14 17:25	DemoZoneNB4	BoDa		Скачать входные цены.xlsx ↓	PrintDoc →	1	8.2 Kb	
2020-06-14 16:47	DemoZoneNB3	d.borislavskiy	 explorer.exe	Скачать Входные цены.xlsx ↓	FileOperation →		8.2 Kb	
2020-06-14 16:01	DemoZoneVM2	Ксения	 chrome.exe	Скачать Входные цены.xlsx ↓	Mail →		8.2 Kb	Бориславский Даниил






Фильтр: *цен* в перехваченных файлах

Свойства Уведомления **Фильтр**

Конструктор Сложный запрос Код фильтра

И + Условие Группа условий

Файл Имя файла Содержит цен ✕

 Перехваченный файл	DemoZoneVM2	Ксения	 skype.exe	Ищем директора Отчёт 2 кв.docx Скачать Отчёт 2 кв.docx ↓ 8:live:..cid.2ba49cc565661352 Ежеквартальный отчёт для директора Тут какие-то очень важные данные Im →
 Перехваченный файл	DemoZoneVM1	Арсений	 thunderbird.exe	Ищем директора Картиночка.jpg  <small>Картина про директора</small> Скачать Картиночка.jpg ↓ Ксения Касперова Картина про директора Mail →

Посещение сайтов

Пользователь: Полное имя	Дата: День	Сайт	Время активности
Арсений Есетовский	18-июнь-2020	searchinform.ru	00 ч 02 м 55 с

Всего: 1, Время активности: 00 ч 02 м 55 с

Переписка - количество

Пользователь: Полное имя	Дата: День	Переписка: Домен получателя	Количество событий
Арсений Есетовский	18-июнь-2020	searchinform.ru	1

Всего: 1, Количество событий: 1

Переписка - подробно


Время	Тип	Компьютер	Пользователь	Приложение	Событие
2020-06-18 10:47:23	Почта	DemoZoneVM1	Арсений	thunderbird.exe	Офис в Новосибирске Арсений Есетовский Добрый день. Подскажите, у вас в Новосибирске офис остался? Или сейчас только в Москве??

Дата	Имя	Заголовок	Контент
2020-06-18 10:37:1	DemoZoneVM2 Ксения	Ксения Касперов r.frank@staffcop.ru Вам нужен офис-менеджер?	
2020-06-14 16:36:1	DemoZoneVM2 Ксения	Ксения Касперов pv@staffcop.ru После вебинара по линукс агенту	
2020-06-14 16:08:1	DemoZoneVM2 Ксения	Ксения Касперов Бориславский Да Re: Данные	
2020-06-14 16:05:0	DemoZoneVM2 Ксения	Ксения Касперов Арсений Есетовс Re: Проверка связи	
2020-06-14 16:01:1	DemoZoneVM2 Ксения	Ксения Касперов Бориславский Да Данные	Скачать Входные цены.xlsx InterceptedFile
2020-06-14 15:45:3	DemoZoneVM2 Ксения	Ксения Касперов Арсений Есетовс Re: Проверка связи	Скачать Лист Microsoft Excel.xlsx InterceptedFile
2020-06-14 15:44:1	DemoZoneVM2 Ксения	Ксения Касперов Арсений Есетовс Проверка связи	

Пользователь: Полное имя	Сайт	Приложение: Заголовок окна	Количество событий
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
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
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
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


Отчеты

Арсений




08.07.2020 12:47:12

Арсений




08.07.2020 12:47:04

Арсений




08.07.2020 12:46:15

Арсений




08.07.2020 12:46:06

Арсений




08.07.2020 12:45:49

Арсений



08.07.2020 12:45:22


Арсений



08.07.2020 12:45:07

Всего: 11, Количество событий: 24

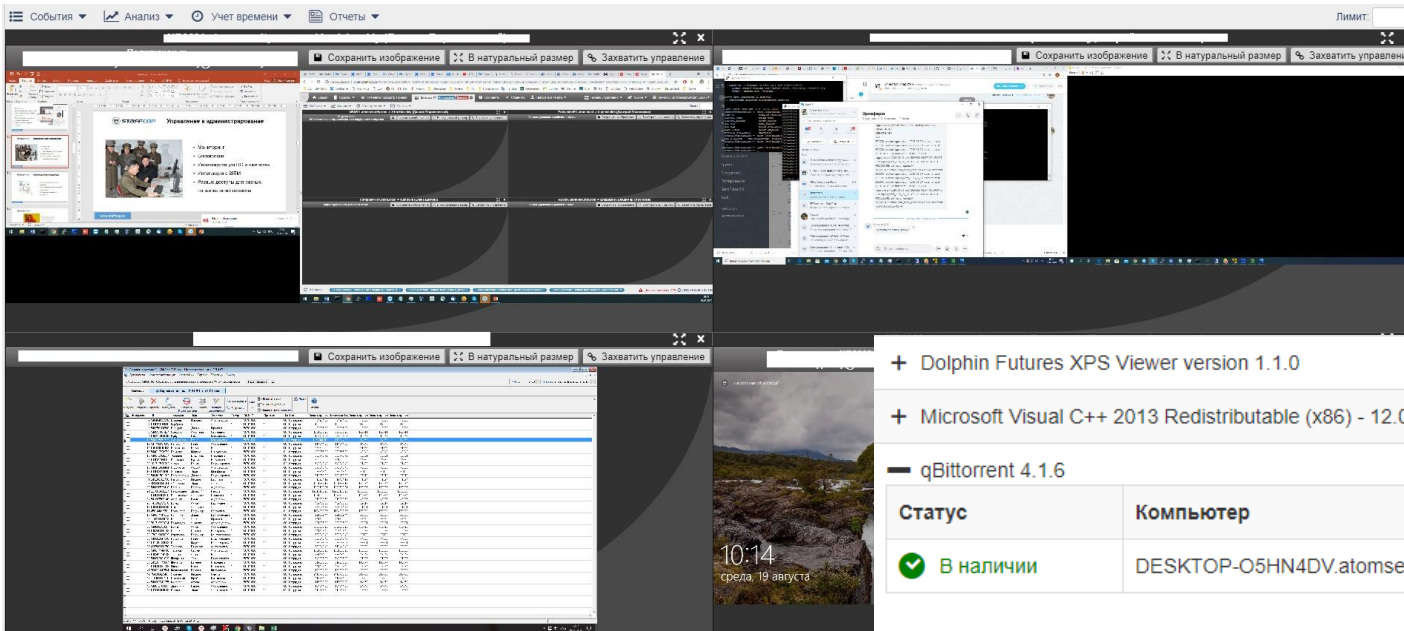


DemoZoneVM2	Ксения	 chrome.exe	<p>Скачать Documents.7z ↓</p> <p>Кредитные карты</p> <p>Ксения Касперова</p> <p>Сначала деньги, потом остальное</p> <p>4276160971368577 сбер</p> <p>вс, 14 июн. 2020 г. в 16:06, Даниил Бориславский <d.borislavskiy@staffcop.ru>: норм, давай ещё</p> <p>вс, 14 июн. 2020 г.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

Время	Тип	Компьютер	Приложение	Событие
2020-01-28 12:13:00	✓ Время активности	NB0201.atomsecurity.c	chrome.exe	Сайты по трудоустройству Вакансия Ведущий программист в Новосибирске, работа в ФГБУ НМИЦ им. ак. Е.Н. Мещалина Минздрава России - Google Chrome https://koltsovo.hh.ru/vacancy/34583944
2020-01-17 16:13:15	✓ Время активности	NB0201.atomsecurity.c	chrome.exe	Сайты по трудоустройству Вакансия Ведущий программист в Новосибирске, работа в ФГБУ НМИЦ им. ак. Е.Н. Мещалина Минздрава России - Google Chrome https://koltsovo.hh.ru/vacancy/34583944
2020-01-17 16:13:09	✓ Время активности	NB0201.atomsecurity.c	chrome.exe	Сайты по трудоустройству Вакансия Ведущий программист в Новосибирске, работа в ФГБУ НМИЦ им. ак. Е.Н. Мещалина Минздрава России - Google Chrome https://koltsovo.hh.ru/vacancy/34583944
2020-01-17 16:11:47	✓ Время активности	NB0201.atomsecurity.c	chrome.exe	Сайты по трудоустройству Вакансия Ведущий программист в Новосибирске, работа в ФГБУ НМИЦ им. ак. Е.Н. Мещалина Минздрава России - Google Chrome https://koltsovo.hh.ru/vacancy/34583944?query=мещалина
2020-01-17 16:11:10	✓ Время активности	NB0201.atomsecurity.c	chrome.exe	Сайты по трудоустройству

Время 2020-01-28 12:13:00
Приложение chrome.exe
Фильтр Сайты по трудоустройству
Тип события ✓ Время активности
Агент NB0201.atomsecurity.com
Пользователь d.borislavskiy
Посещение сайта <https://koltsovo.hh.ru/vacancy/34583944>
Домен hh.ru
Сайт koltsovo.hh.ru
Заголовок окна Вакансия Ведущий программист в Новосибирске
Длительность 00:00:30
Содержимое <https://koltsovo.hh.ru/vacancy/34583944>
PID 5096

Посещение сайтов по трудоустройству				Выгрузка и печать	Панель управления	Админ	Меню (Admin)
Пользователь: Полное имя	Сайт	Дата: День	Время активности				
Ксения Касперова	hh.ru	14-июнь-2020	00 ч 07 м 44 с				
Ксения Касперова	hh.ru	18-июнь-2020	00 ч 04 м 35 с				
Ксения Касперова	superjob.ru	18-июнь-2020	00 ч 03 м 02 с				
Ксения Касперова	job.ru	18-июнь-2020	00 ч 00 м 20 с				
				Всего: 4, Время активности: 00 ч 15 м 39 с			



+ Dolphin Futures XPS Viewer version 1.1.0

+ Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40649

— qBittorrent 4.1.6

Статус	Компьютер	Поставщик	Версия	Дата наличия
✔ В наличии	DESKTOP-O5HN4DV.atomsecurity.com	The qBittorrent project	4.1.6	17:06:25 04.06.2020

+ Update for Microsoft Office 2013 (KB3039756) 32-Bit Edition

+ Update for Microsoft Office 2010 (KB4092436) 32-Bit Edition

+ K-Lite Codec Pack 14.1.5 Full

— Git version 2.22.0.windows.1

Статус	Компьютер	Поставщик	Версия	Дата наличия
✔ В наличии	NB0001.atomsecurity.com	The Git Development Community	2.22.0.windows.1	18:29:13 21.01.2020

+ Обновление безопасности для Windows XP (KB2820917)

+ Обновление безопасности для Windows XP (KB976323)

Потребители





На open source решениях и не требует дополнительного платного программного обеспечения.



Бессрочные лицензии и гибкая политика лицензирования.



OLAP-куб снижает требования к «железу» сервера.



97% внедрений StaffCop окупилась менее чем за 2 месяца.



Полноценное техническое сопровождение с начального этапа тестирования.



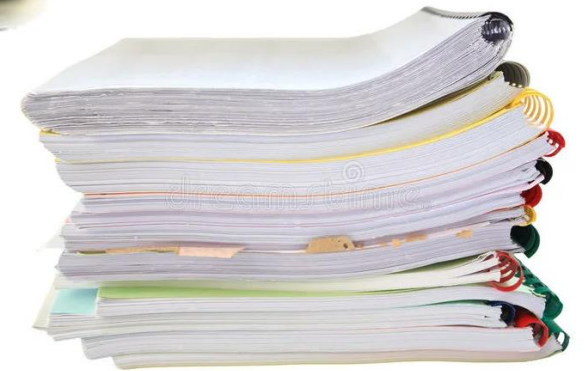
Многомерные аналитические отчёты и схемы с возможностью перехода от общего к частному и наоборот.

Аспекты внедрения

Правовые

Технические

Административные



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

- В дополнение к лицензиям на ПО могут потребоваться лицензии на OS и DataBase.
- Развёртывание и настройка системы.
- Система не должна мешать бизнесу работать и зарабатывать.
- Не платите за то, что вам не нужно.
- Возможно, потребуется сертифицированная ФСТЭК версия.
- Система должна иметь возможность быть полезной всем подразделениям.
- Система должна решать задачи поставленные бизнесом.

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



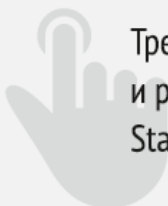
Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро



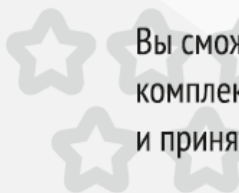
Развертывание пилотного проекта обычно занимает не более одного дня

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!

Даниил Бориславский
Руководитель аналитического отдела
ООО Атом Безопасность

 +7(499)6382809 доб. 235
 db@staffcop.ru
 d.borislavskiy