



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



Даниил Бориславский
Аналитик ИБ, специалист
по внедрению
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»
- ~100 серверных компонентов в месяц; ~ 94 000 АРМ за 2019-й год.



Технопарк Новосибирского Академгородка



ФСТЭК России
Федеральная служба
по техническому и
экспортному контролю



Минкомсвязь
России



STAFFCOP

Зачем нужен контроль над инф.потоками?

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 ₺

[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

Подписаться на продавца





Контроль сотрудников на удалёнке

События Анализ Учет времени Отчеты

Лимит:

Учёт рабочего времени за период с 24 марта 2020 по 24 марта 2020

24 марта 2020 г. Вторник

Пользователь ↓	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 ↓	Опоздание ↓	Сверхурочные ↓	Продуктивное ↓	Непродуктивное ↓	Нейтральное ↓
		8:07:07	20:08:51	12ч 01м 44с	6ч 12м 31с	5ч 49м 13с	00с	1ч 09м 21с	00с	6ч 12м 31с	00с
Продуктивность											
Развлекательные ресурсы		6:12:53 (100.10%)									
Топ приложений											
chrome.exe		6:12:53 (100.10%)									
Топ сайтов											
youtube.com		5:40:29 (91.40%)									
twitch.tv		0:32:24 (8.70%)									

Подробный отчет по активности с 24 Мар 2020 по 24 Мар 2020

[Скачать файлы в ZIP архиве](#)

	Дата	Компьютер	Пользователь	Приложение	Затраченное время	Домен	Заголовок
+ 54	19:56:56 24.03.2020			chrome.exe	00:35:21	youtube.com	● Прохождение Half-Life: Alyx в шлеме Valve Index #1 - YouTube - Google Chrome
	18:46:52 24.03.2020			chrome.exe	00:00:02	youtube.com	utq follower - YouTube - Google Chrome
+ 4	18:46:46 24.03.2020			chrome.exe	00:02:45	youtube.com	YouTube - Google Chrome
+ 3	18:41:56 24.03.2020			chrome.exe	00:02:17	youtube.com	Assassin's Creed Syndicate Cinematic Trailer - YouTube - Google Chrome
+ 2	18:39:41 24.03.2020			chrome.exe	00:01:14	youtube.com	YouTube - Google Chrome
+ 5	18:38:37 24.03.2020			chrome.exe	00:03:36	youtube.com	VK FEST 2017. Макс Корж - Малый повзрослел. - YouTube - Google Chrome
	18:33:57 24.03.2020			chrome.exe	00:00:34	youtube.com	YouTube - Google Chrome
+ 3	18:33:19 24.03.2020			chrome.exe	00:02:37	youtube.com	Танцующий Волк-романтик оставил судей "Маски" почти без вариантов! - YouTube - Google Chrome
+ 2	18:31:10 24.03.2020			chrome.exe	00:01:09	youtube.com	YouTube - Google Chrome
	18:29:39 24.03.2020			chrome.exe	00:00:30	youtube.com	Играем в Half-Life: Alyx - YouTube - Google Chrome
+ 5	18:28:57 24.03.2020			chrome.exe	00:04:42	youtube.com	Волк стал Волчицей! Смена голоса артиста под серой маской шокировала жюри - YouTube - Google Chrome
+ 4	18:24:50 24.03.2020			chrome.exe	00:01:52	youtube.com	"Маска" — Волк: Dance Monkey - YouTube - Google Chrome
	18:22:48			chrome.exe	00:00:04	youtube.com	wolf dance monkey - YouTube - Google Chrome



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



учет рабочего
времени



эффективность
персонала



информационная
безопасность

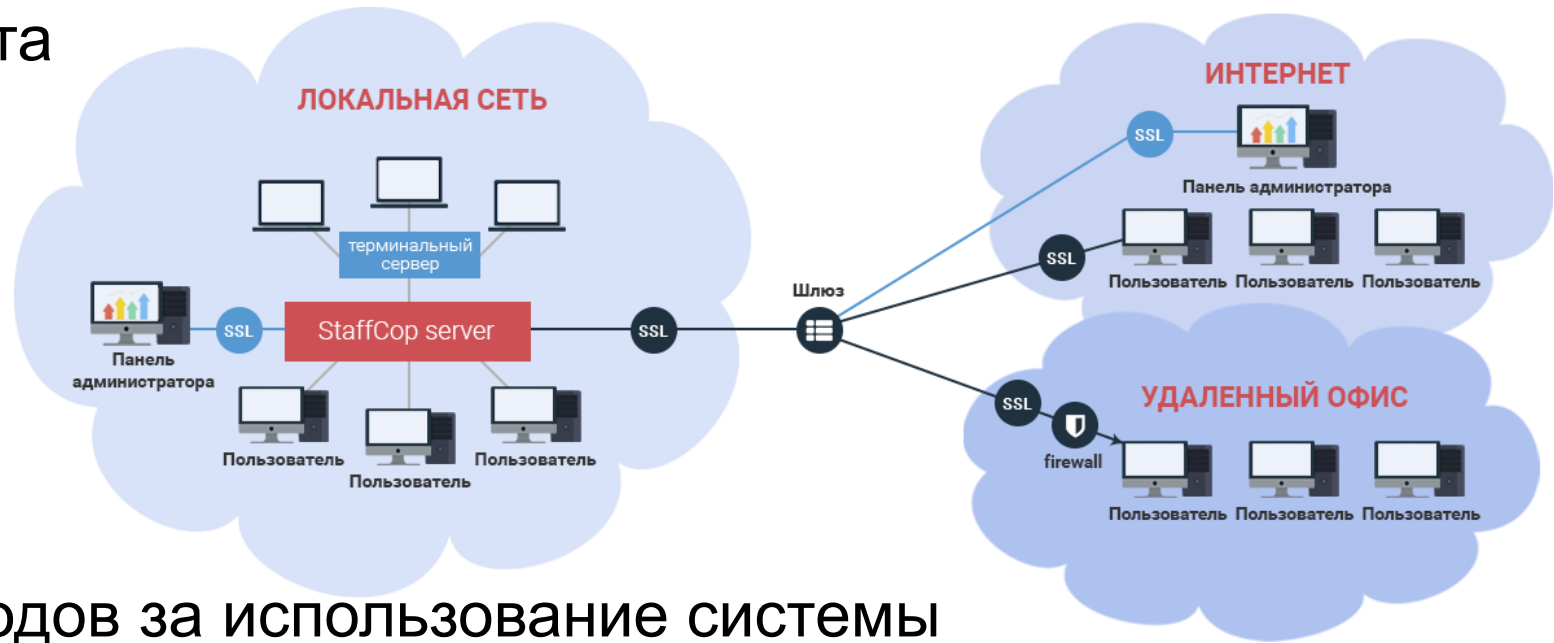


расследование
инцидентов



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




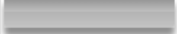






00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	Начало ↓	Окончание ↓	Общее время ↓	Активное ↓	Простой ↓
																								9:54:29	21:15:32	11:21:03	6:14:19	5:06:44
																								9:07:06	18:22:55	9:15:49	8:34:07	0:41:42
																								11:20:35	20:01:01	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

Отчет по активности пользователей за период с 1 июня 2020 по 30 июня 2020

Даниил Бориславский						
Пользователь	Общее время	Активное время	Время простоя	Опоздание	Сверхурочные	Продуктивн
Даниил Бориславский	245:46:59	106:55:53	138:51:06	27:50:19	6:01:37	
— Продуктивность						
Офисные приложения	23:54:58 (22.37%)					
Поисковые порталы	17:01:07 (15.92%)					
Приложения для удаленного доступа	14:40:02 (13.72%)					
Всё остальное	13:41:09 (12.80%)					
Корпоративные ресурсы	11:59:14 (11.21%)					
Интернет-мессенджеры	7:24:04 (6.92%)					
Корп. ресурсы	5:45:15 (5.38%)					
Почтовые приложения	4:34:14 (4.27%)					
Информационная безопасность	2:02:01 (1.90%)					
Интерфейс системы	1:22:53 (1.29%)					
+ Топ приложений						
+ Топ сайтов						

Учёт рабочего времени за период с 22 июня 2020 по 28 июня 2020

22 июня 2020 г. Понедельник																													
Пользователь ↓	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 ↓	
Даниил Бориславский																										9:15:55	21:14:42	11:58:47	4:27:33
23 июня 2020 г. Вторник																													
Пользователь ↓	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 ↓	
Даниил Бориславский																										9:24:34	21:32:22	12:07:48	4:05:19
24 июня 2020 г. Среда																													
Пользователь ↓	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 ↓	
Даниил Бориславский																										10:37:05	22:34:43	11:57:38	0:32:47
25 июня 2020 г. Четверг																													
Пользователь ↓	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 ↓	
Даниил Бориславский																										8:58:03	21:41:56	12:43:53	6:40:55
26 июня 2020 г. Пятница																													
Пользователь ↓	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 ↓	
Даниил Бориславский																										12:13:23	22:56:19	10:42:56	4:03:16

Почасовая оплата работы у заказчика

меню Отчеты Лимит:

Приложение: Название	Приложение: Описание	Время активности
bitrix24.exe	Значение не указано	14:53:53
winword.exe	Microsoft Word	03:43:59
powerpnt.exe	Microsoft PowerPoint	03:04:20
excel.exe	Microsoft Excel	01:17:06

	9	10	11	12	13	14	15					
Вход	9:23:06	9:38:04	9:46:13	14:10:01	9:00:02	9:15:01	9:24:42	12:26:53	9:23:14	0:00:00	14:40:31	9:02:51
Выход	19:31:27	20:41:37	18:15:27	20:30:09	19:26:01	20:34:03	19:48:56	18:17:09	21:31:26	23:31:20	19:33:31	19:45:17
Время нахождения в офисе	4:22:24	4:46:42	5:54:53	4:16:31	6:24:36	5:26:39	6:17:36	4:46:13	4:45:29	0:00:07	0:46:41	5:56:56
Время работы в разрешенном ПО	1:54:46	1:43:38	1:53:18	1:08:39	3:27:05	2:17:49	2:16:09	1:24:15	1:41:52	0:00:00	0:39:39	2:22:22
Время работы в запрещенном ПО	0:04:56	0:00:50	0:00:36	0:02:42	0:01:23	0:02:24	0:01:29	0:09:28	0:00:10	0:00:00	0:00:00	0:00:00
Простой	5:45:57	6:16:51	2:34:21	2:03:37	4:01:23	5:52:23	4:06:38	1:04:03	7:22:43	23:31:13	4:06:19	4:45:30

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

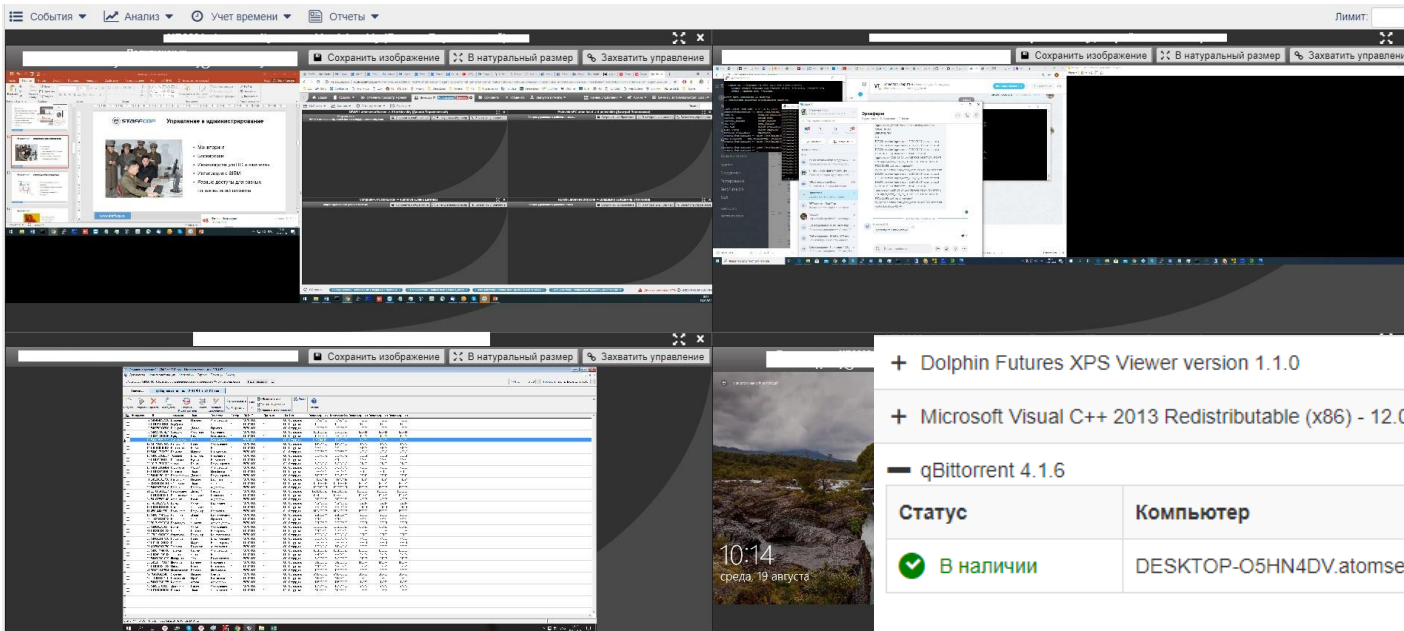
Посещение сайтов по трудоустройству				Выгрузка и печать		Панель управления		Админ		Меню (Admin)	
Пользователь: Полное имя	Сайт	Дата: День	Время активности								
Ксения Касперова	hh.ru	14-июнь-2020	00 ч 07 м 44 с								
Ксения Касперова	hh.ru	18-июнь-2020	00 ч 04 м 35 с								
Ксения Касперова	superjob.ru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

Время	Тип	Пользователь	Приложение	Событие
2019-12-04 17:58:38	Интернет-пейджер	Ксения	skype.exe	8:live:.cid.2ba49cc565661352 Я, наверное, сначала договорюсь с новой работой, а затем напишу заявление и возьму сразу больничный
2019-12-04 17:58:02	Интернет-пейджер	Ксения	skype.exe	8:live:.cid.2ba49cc565661352 Но он поди мне рекомендацию даст плохую, если я уволюсь
2019-12-04 17:57:43	Интернет-пейджер	Ксения	skype.exe	8:live:.cid.2ba49cc565661352 Я пошла искать работу
2019-12-04 17:57:35	Интернет-пейджер	Ксения	skype.exe	8:live:.cid.2ba49cc565661352 Сегодня сказал что я должна печатать слепым методом, а не так как я сейчас
2019-12-04 17:57:10	Интернет-пейджер	Ксения	skype.exe	8:live:.cid.2ba49cc565661352 Сеня, задолбал меня наш debil

chrome.exe
Выгруженные через браузер файлы
Re: По делам
Годовой отчёт.rtf
Скачать Годовой отчёт.rtf [↓](#)
Ксения
Здесь данные за год.
От генерального **директора**
А также много картинок и цифр
Mail [↔](#)

thunderbird.exe
Ищем директора
Re: Письмецо
Ксения
ХЗ. **директор** может посту**вить** как мудака 23.04.2020 14:54, Ксения Касперова пишет: > Сеня, говорят, что после самоизоляции нас так и оставят из дома > работать, чтоб аренду не платить. Знаешь подробности?

Время 2020-04-23 15:05:56
Приложение **thunderbird.exe**
Фильтр Ищем директора
Тип события **Почта**
Агент DemoZoneVM1 (1.41)
Пользователь Арсений
Отправитель **Ксения**
Получатели **Ксения** [+](#)
Участники **Ксения** [▶](#) **Ксения**
Формат Plain
Заголовок окна Re: Письмецо
Содержимое ХЗ. **директор** может посту**вить** как мудака 23.04.2020 14:54, Ксения Касперова пишет:
> Сеня, говорят, что после самоизоляции нас так и оставят из дома
> работать, чтоб аренду не платить. Знаешь подробности?
PID 1904



+ 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)

Общение с конкурентами и личная почта

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??

Лимит:

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	

Обнаружили запись файла на флэшку	Выгрузка и печать	Панель управления					
События	Анализ	Учет времени	Отчеты				
Время	Компьютер	Пользователь	Приложение	Контент	Связано с	Страницы	Размер
2020-06-14 16:47	DemoZoneNB3	d.borislavskiy	explorer.exe	Скачать Входные цены.xlsx	FileOperation		8.2 Kb

Где подключали флэшку	Выгрузка и печать	Панель управления	Адм
События	Анализ	Учет времени	Отчеты
Агент: Компьютер	Пользователь: Полное имя	Дата: День	Устройство
DemoZoneNB3	Бориславский Даниил	14-июнь-2020	JetFlash Transcend 16GB USB Device
DemoZoneNB4	BoDa	14-июнь-2020	JetFlash Transcend 16GB USB Device

Файл не в том месте	
События	Ана
Пользователь: Полное имя	
Арсений Есетовский	

Арсений Есетовский	winword.exe	значение не указано	\\demozonevm1\Новая папка\
Арсений Есетовский	winword.exe	Для Лены.docx	C:\Users\Арсений\Desktop\Для Лены.docx
Арсений Есетовский	winword.exe	Проект_28.docx	\\Demozonevm1\Новая папка\Проект_28.docx
Арсений Есетовский	winword.exe	Проект_28.docx	\\Demozonevm1\Новая папка\Проект_28.docx
Арсений Есетовский	winword.exe	проект_9.docx	C:\Users\Арсений\Documents\проект_9.docx



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 окупались 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.

Правовые



Технические



- Рабочее – это рабочее, личное – это личное.
- ДС в трудовой договор.
- Приказ о введении автоматизированного контроля.

- *Приказ о переводе на удалённую работу с контролем.
- *Акт приёма-передачи ТМЦ.

- **№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



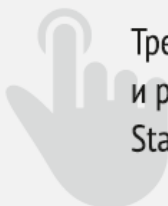
Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро



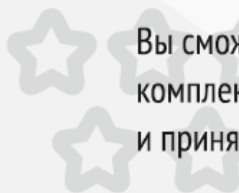
Развертывание пилотного проекта обычно занимает не более одного дня

Легко



Требуется минимум усилий и ресурсов для запуска StaffCop Enterprise

Комплексно






Вы сможете оценить сразу весь комплекс решаемых задач и принять правильное решение



Спасибо за внимание!

Даниил Бориславский
Аналитик ИБ, специалист по внедрению
ООО Атом Безопасность

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