



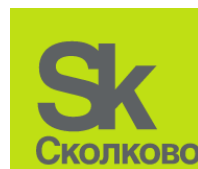
**Контроль над информационными потоками
и действиями сотрудников в рамках работы из офиса и
удаленно.**

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

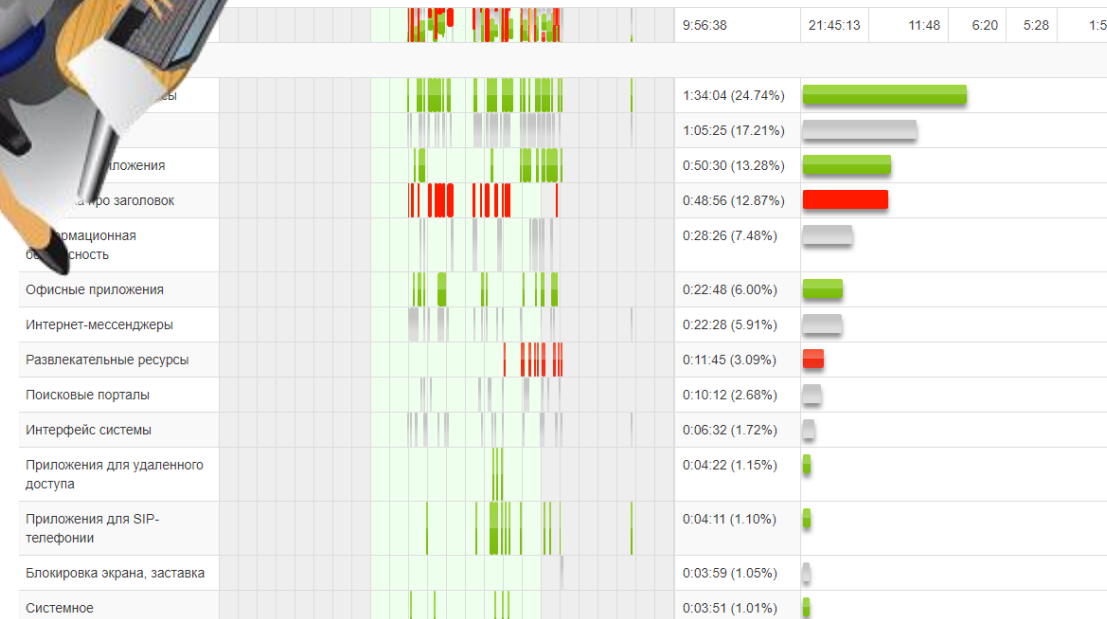


ФСТЭК России
Федеральная служба
по техническому и
экспортному контролю

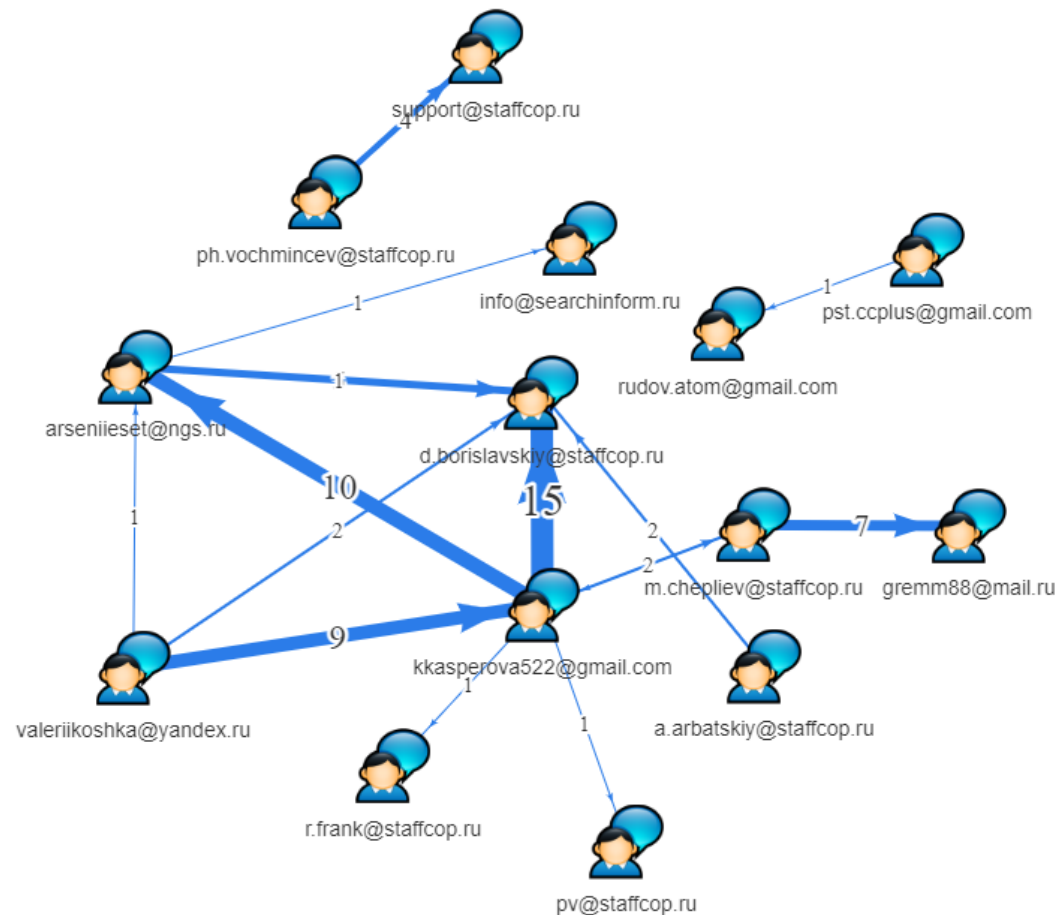


Минкомсвязь
России



[illegible]

С кем он работает? Карта взаимодействий и переписка.



Что?

С чем он работает? Оборудование, ПО и файлы.



Зачем?

Чтобы обезопасить работника и работодателя.



Зачем?

Чтобы повысить эффективность и рабочего процесса и его организации.



Зачем?

Обязаны по законодательству.



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.

Как контролировать тех кто в офисе?



Продуктивное время за период с 8 февраля 2021 по 8 февраля 2021

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

Сотрудник	Отработанное	Продуктивное	Непродуктивное	Нейтральное
По всем отделам (10)		28:45:10 (52,69 %)	1:56:43 (3,56 %)	23:52:35 (43,75 %)
▼ Техническая Поддержка (10)		28:45:10 (52,69 %)	1:56:43 (3,56 %)	23:52:35 (43,75 %)
Максим		5:15:41 (61,05 %)	0:01:45 (0,34 %)	3:19:37 (38,61 %)
Даниил		4:49:46 (66,08 %)	0:36:09 (8,24 %)	1:52:37 (25,68 %)
Владимир		4:40:12 (60,74 %)	0:00:00 (0,0 %)	3:01:07 (39,26 %)
Юрий		4:28:38 (78,15 %)	0:00:00 (0,0 %)	1:15:06 (21,85 %)
Сергей		3:16:07 (47,13 %)	0:00:00 (0,0 %)	3:40:00 (52,87 %)
Филипп		2:35:04 (48,51 %)	1:12:01 (22,53 %)	1:32:36 (28,97 %)
Александр		1:54:38 (25,55 %)	0:00:16 (0,06 %)	5:33:41 (74,39 %)
Дмитрий		1:29:52 (33,0 %)	0:00:00 (0,0 %)	3:02:27 (67,0 %)
Анатолевич		0:14:54 (36,56 %)	0:00:00 (0,0 %)	0:25:51 (63,44 %)
Филипп		0:00:18 (1,83 %)	0:06:32 (39,88 %)	0:09:33 (58,29 %)

Начало	Окончание	Общее время	Активное	Простой	Опоздание	Сверхурочные	Продуктивное	Непродуктивное	Нейтральное
10:24:50	20:07:58	8:43	6:48	1:54	1:24	0:18	4:46	0:01	1:59
9:25:52	18:31:41	9:05	7:02	2:03	1:25	1:19	4:16	0:28	1:33

Как контролировать тех кто работает удаленно?



	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20			
Philip Vochmincev																								
Бориславский Даниил																								
15 июля 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
Philip Vochmincev																								
Бориславский Даниил																								

- **№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.



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



учет рабочего
времени



эффективность
персонала



информационная
безопасность

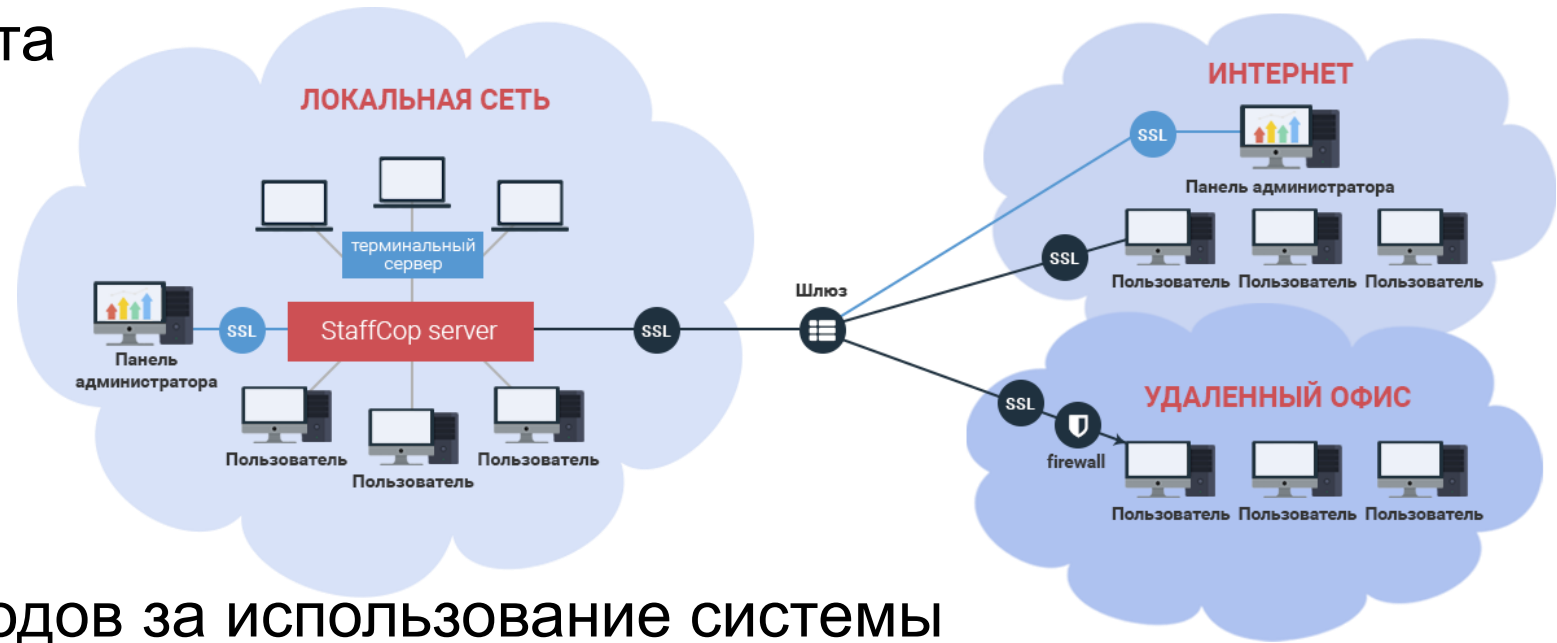


расследование
инцидентов



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

Тотальный контроль действий за ПК



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



1. RDP до рабочего ПК.
2. RDP до терминального сервера.
3. Рабочий ноутбук дома + VPN.
4. Рабочий ноутбук дома и нет VPN.
5. Только VPN.
6. Отсутствует какой либо доступ

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



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



Управление и администрирование

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

Учёт рабочего времени на удалёнке

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						

Почасовая оплата работы у заказчика

Имени: 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

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



Расследование инцидентов

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 ▾ ⚙ Адми					
События ▾ Анализ ▾ Учет времени ▾ Отчеты ▾					
Агент: Компьютер ▾ ⚙	Пользователь: Полное имя ▾ ⚙	Дата: День ▾ ⚙	Устройство ▾ ⚙		
DemoZoneNB3	Бориславский Даниил	14-июнь-2020	JetFlash Transcend 16GB USB Device	2	
DemoZoneNB4	BoDa	14-июнь-2020	JetFlash Transcend 16GB USB Device	1	

Файл не в том месте
События ▾ Ана
Пользователь: Полное имя ▾

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



Теневые копии файлов – Поиск по атрибутам и анализ содержимого.

Время	Компьютер	Пользователь	Приложение	Контент	Связано с	Страницы	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

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

Фильтр: *цен* в перехваченных файлах

Свойства

Уведомления

Фильтр

Конструктор

Сложный запрос

Код фильтра

И

Условие

Группа условий

Файл

Имя файла

Содержит

цен

Перехваченный файл	DemoZoneVM1	Арсений	thunderbird.exe
--------------------	-------------	---------	-----------------

Ищем директора
Картиночка.jpg

Скачать Картиночка.jpg
Ксения Касперова
Картина про директора
Mail



Контроль переписки - общение с конкурентами.

Общение с конкурентами					
Выгрузка и печать					
Панель управления					
Админ					
Меню (Admin)					
События					
Анализ					
Учет времени					
Отчеты					
Добавить					
Лимит:					
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??					
2020-06-14 16:08:11					
DemoZoneVM2					
Ксения					
Ксения Касперов					
Бориславский Да					
2020-06-14 16:05:00					
DemoZoneVM2					
Ксения					
Ксения Касперов					
Арсений Есетовс					
2020-06-14 16:01:11					
DemoZoneVM2					
Ксения					
Ксения Касперов					
Бориславский Да					
2020-06-14 15:45:33					
DemoZoneVM2					
Ксения					
Ксения Касперов					
Арсений Есетовс					
2020-06-14 15:44:11					
DemoZoneVM2					
Ксения					
Ксения Касперов					
Арсений Есетовс					

Панель управления	
Админ	
Меню (Admin)	
Лимит:	
Заголовок	Контент
Вам нужен офис-менеджер?	
После вебинара по линукс агенту	
Re: Данные	
Re: Проверка связи	
Данные	Скачать Входные цены.xlsx InterceptedFile
Re: Проверка связи	Скачать Лист Microsoft Excel.xlsx InterceptedFile
Проверка связи	

Доски объявлений – продажа оборудования.

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

Всего: 11, Количество событий: 24

Отчеты



08.07.2020 12:47:12

Арсений



Арсений



08.07.2020 12:47:04



Арсений



08.07.2020 12:46:15

Арсений



08.07.2020 12:46:06



08.07.2020 12:45:49



08.07.2020 12:45:22

Арсений



08.07.2020 12:45:07

Сканы паспортов и номера кредитных карт – инцидент?

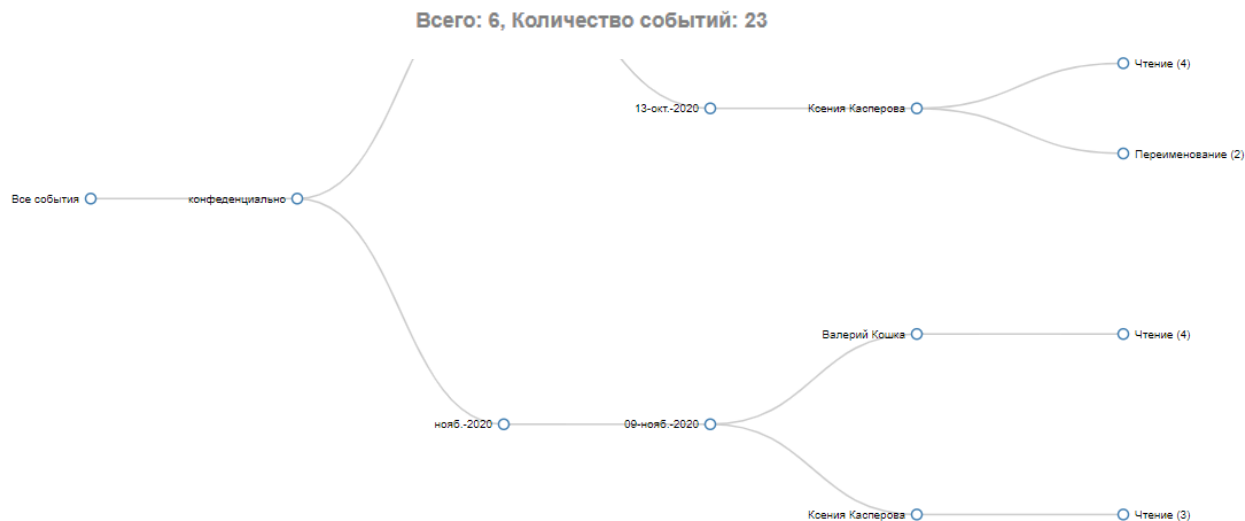


DemoZoneVM2	Ксения	 chrome.exe	Скачать Documents.7z ↓ Кредитные карты Ксения Касперова Сначала деньги, потом остальное 4276160971368577 сбер вс, 14 июн. 2020 г. в 16:06, Даниил Бориславский <d.borislavskiy@staffcop.ru>: норм, давай ещё вс, 14 июн. 2020 г. в 16:01, Ксения Касперова <kkasperova522@gmail.com>: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

Метки на файлы

Файл: Метка	Дата: Месяц	Дата: День	Пользователь: Полное имя	Файл: Операция	Количество событий
конфиденциально	нояб.-2020	09-нояб.-2020	Валерий Кошка	Чтение	4
конфиденциально	нояб.-2020	09-нояб.-2020	Ксения Касперова	Чтение	3
конфиденциально	окт.-2020	12-окт.-2020	Валерий Кошка	Перезапись	1
конфиденциально	окт.-2020	12-окт.-2020	Валерий Кошка	Чтение	9
конфиденциально	окт.-2020	13-окт.-2020	Ксения Касперова	Переименование	2
конфиденциально	окт.-2020	13-окт.-2020	Ксения Касперова	Чтение	4

↑ x Файл: Операция ↓ ↑ x + Колич'





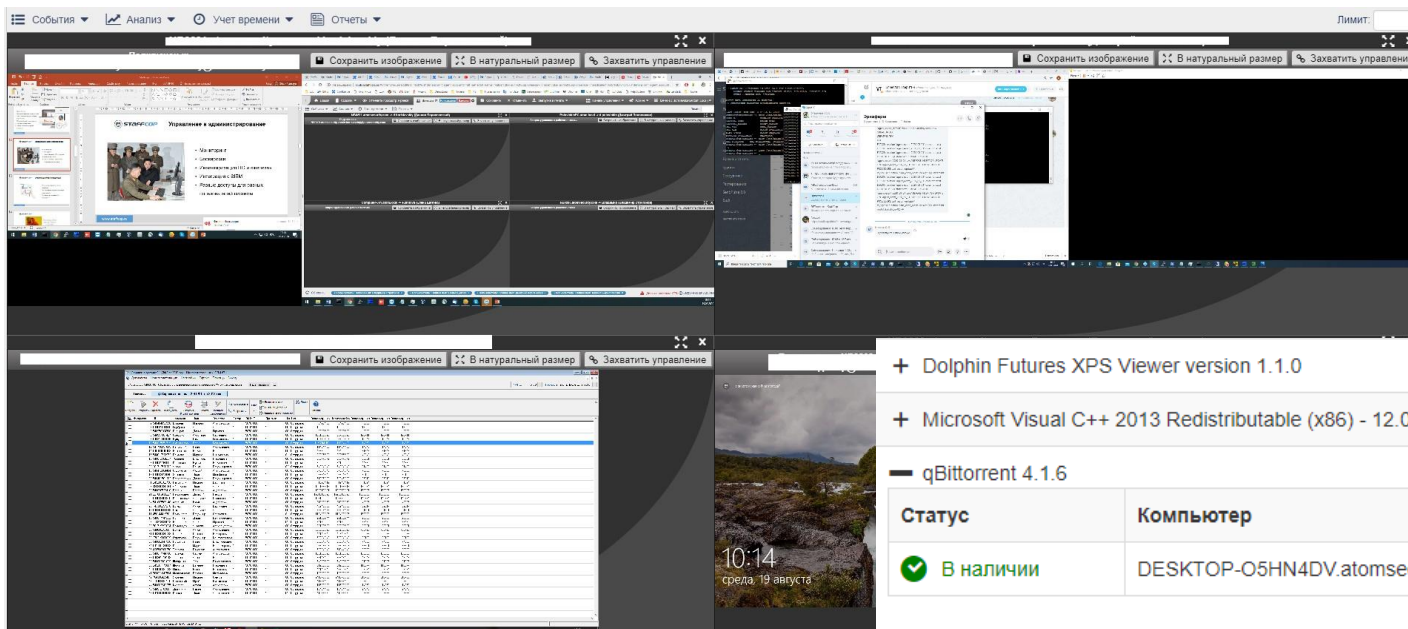
Отслеживание поиска работы и эмоциональная обстановка в офисе.

2020-04-23 15:09:14	Перехваченный	DemoZoneVM2 (1.27)	Ксения	chrome.exe
2020-04-23 15:05:56	Почта	DemoZoneVM1 (1.41)	Арсений	thunderbird.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

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
Формат Plain
Заголовок окна Re: Письмецо
Содержимое
ХЗ. Директор может поступить 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

Посещение сайтов по трудоустройству				Выгрузка и печать	Панель управления	Админ	Меню (Admin)
События	Анализ	Учет времени	Отчеты	Лимит:			
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

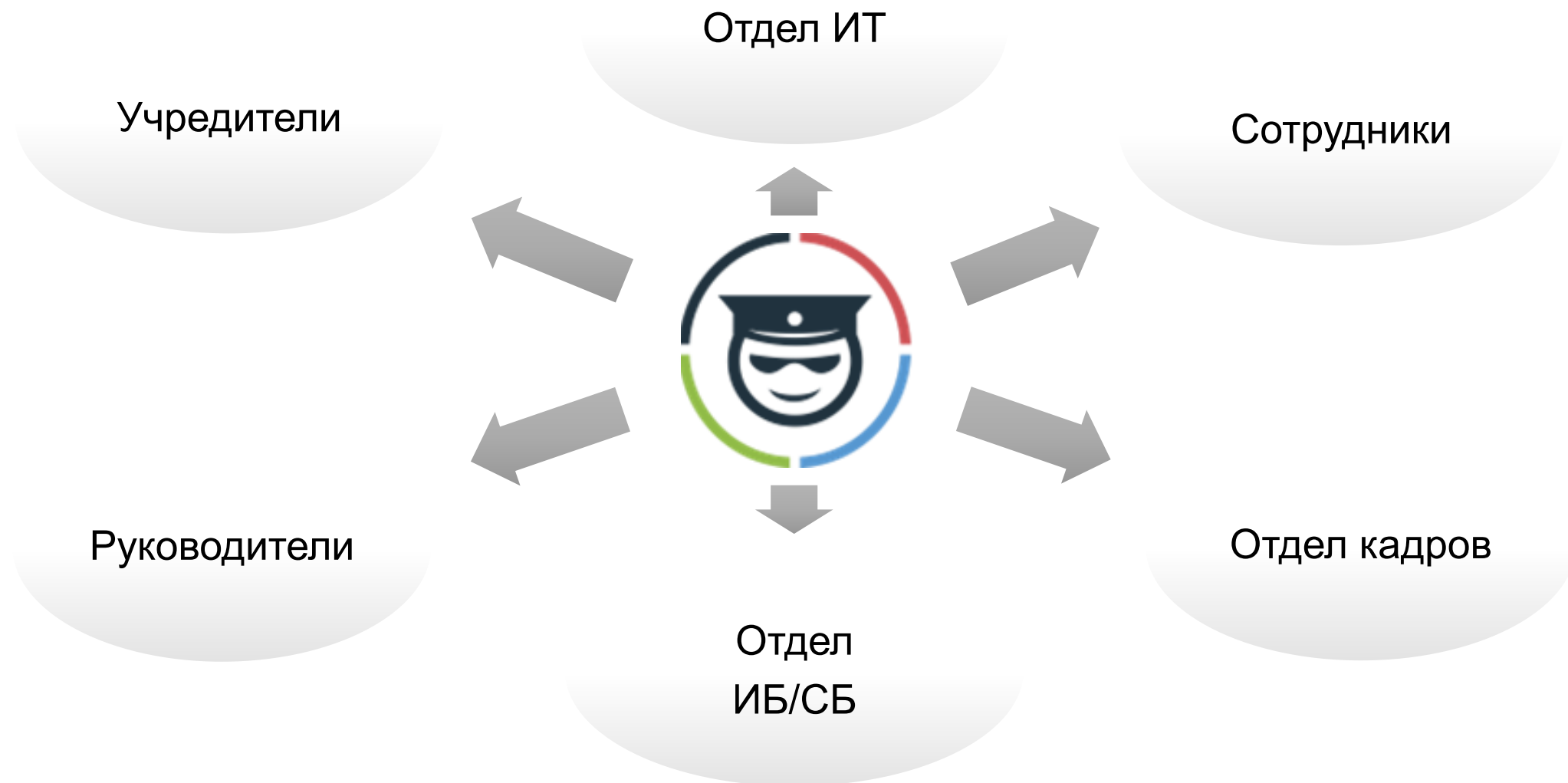
— Git version 2.22.0.windows.1

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)

Кому это может быть полезно?



Почему мы?



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.



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



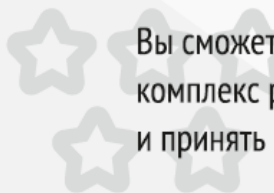
Развертывание пилотного проекта обычно занимает не более одного дня

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