



В поисках девиантного поведения.



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.



Девииантное поведение

Девииантное поведение (также социальная девиация, отклоняющееся поведение) (лат. deviation — отклонение) — это устойчивое **поведение** личности, **отклоняющееся от** общепринятых, наиболее распространённых и устоявшихся общественных **норм**. Негативное девиантное поведение приводит к применению обществом определённых формальных и неформальных санкций (изоляция, лечение, исправление или наказание нарушителя).

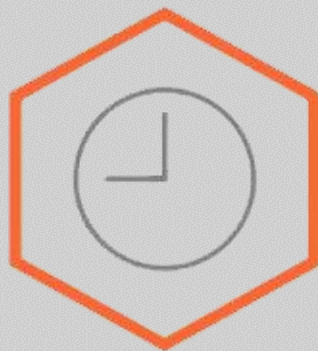
Девииантное поведение

В нашем контексте нужно:

1. Определить что есть допустимая и ожидаемая нормы.
2. Определить как всё есть на самом деле.
3. Определить какие есть отклонение от нормы.
4. Что-то сделать с полученными результатами.
5. PDCA.



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



учет рабочего
времени



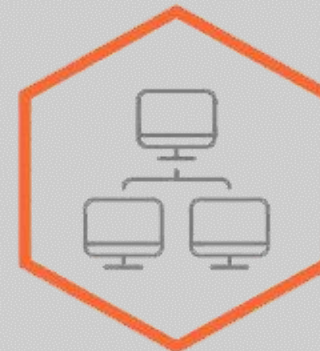
эффективность
персонала



информационная
безопасность



расследование
инцидентов



удаленное
администрирование

Определить как всё есть на самом деле

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

Определить отклонение от нормы

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 ↓	
																									9:39:31	18:35:15	8:55:44	7:23:41
																									11:16:47	19:40:16	8:23:29	5:32:36
																									11:30:44	20:25:27	8:54:43	6:31:18
																									10:14:45	18:19:48	8:05:03	7:02:15
																									10:30:13	18:54:25	8:24:12	6:39:46
																									9:48:31	19:42:57	9:54:26	7:22:04
																									9:11:06	18:16:15	9:05:09	7:52:04
																									10:00:10	18:12:09	8:11:59	7:43:48
																									12:01:48	20:56:05	8:54:17	8:20:02

Определить отклонение от нормы

12 июля 2021 г. Понедельник

[illegible]

13 июля 2021 г. Вторник

[illegible]

14 июля 2021 г. Среда

[illegible]

15 июля 2021 г. Четверг

[illegible]

16 июля 2021 г. Пятница

[illegible]

Определить отклонение от нормы

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	

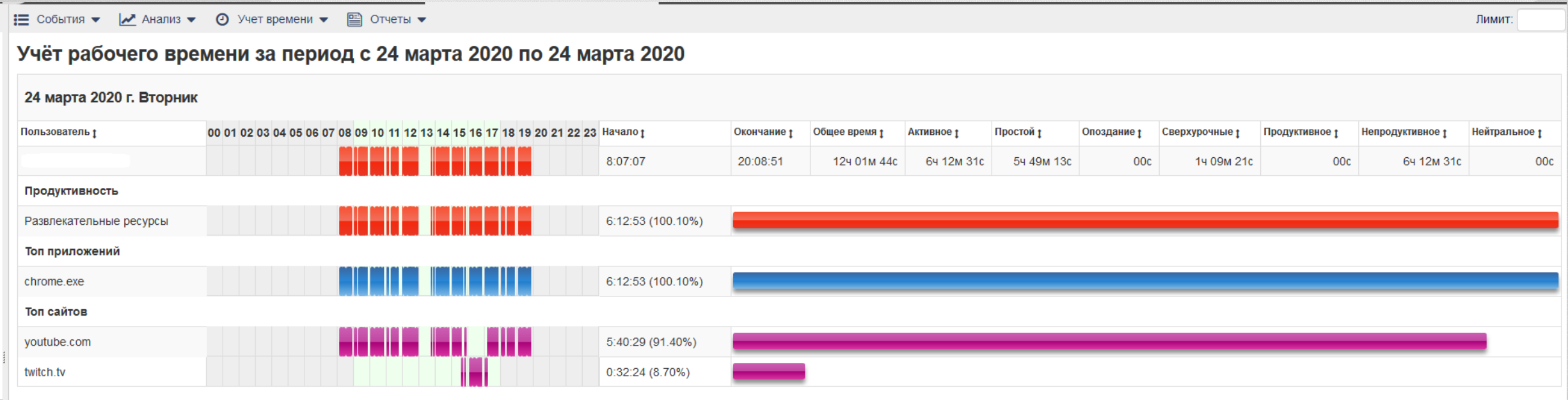
— Продуктивность

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

Определить отклонение от нормы



Определить отклонение от нормы



AliExpress™



Посещение сайтов и поисковые запросы

Сайты отчётности

Изменен

События

Анализ

Учет времени

Отчеты

Лимит:

Пользователь: Полное имя

Сайт

Время активности

Арсений Есетовский	sbis.ru	00 ч 02 м 55 с
Ксения Касперова	nalog.ru	00 ч 02 м 32 с
Ксения Касперова	sbis.ru	00 ч 00 м 43 с

Текст

запада 3 сезон 5 серия

Арсений	firefox.exe	youtube.com	мир дикого запада 3 сезон
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	солитер виндовс 7 скачать бесплатно
Арсений	firefox.exe	yandex.ru	солитер
Арсений	firefox.exe	yandex.ru	солитер
Ксения	chrome.exe	google.com	купить тест на беременность с 2 полосками
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера
Арсений	firefox.exe	yandex.ru	как удалить staffcop с компьютера

Словари

☰ События ▾ | 📈 Анализ ▾ | ⌚ Учет времени ▾ | 📄 Отчеты ▾

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 дебил

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 поступить как мудака 23.04.2020 14:54, Ксения Касперова пишет: > Сеня, говорят, что после самоизоляции нас так и оставляют 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
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 оставляют из дома > работать, чтоб аренду не платить. Знаешь подробности?
PID	1904

Теневые копии файлов – поиск по тексту

 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  Картина про директора Скачать Картиночка.jpg  Ксения Касперова Картина про директора Mail 

Общение с конкурентами и личная почта

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??

Панель управления

Админ

Меню (Admin)

Лимит:

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

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 ▾

Пользователь: Полное имя ▾

Арсений Есетовский

Арсений Есетовский

Арсений Есетовский

Арсений Есетовский

Арсений Есетовский

winword.exe

winword.exe

winword.exe

winword.exe

winword.exe

Значение не указано

Для Лены.docx

Проект_28.docx

Проект_28.docx

проект_9.docx

\\Demozonevm1\Новая папка\

C:\Users\Арсений\Desktop\Для Лены.docx

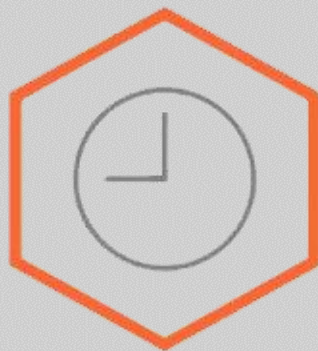
\\Demozonevm1\Новая папка\Проект_28.docx

\\Demozonevm1\Новая папка\Проект_28.docx

C:\Users\Арсений\Documents\проект_9.docx



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



учет рабочего
времени



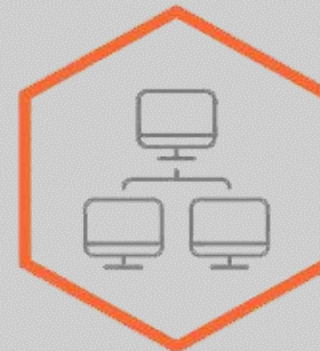
эффективность
персонала



информационная
безопасность



расследование
инцидентов



удаленное
администрирование

Современные архитектурные решения

- 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
 - 100 сотрудников <> 6CPU, 16RAM
 -
- 
- Локальная сеть
- Терминальный сервер
- Консоль управления
- SSL
- Интернет
- Терминальный сервер



- Нет дополнительных расходов за использование системы

Тотальный контроль действий за ПК

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



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

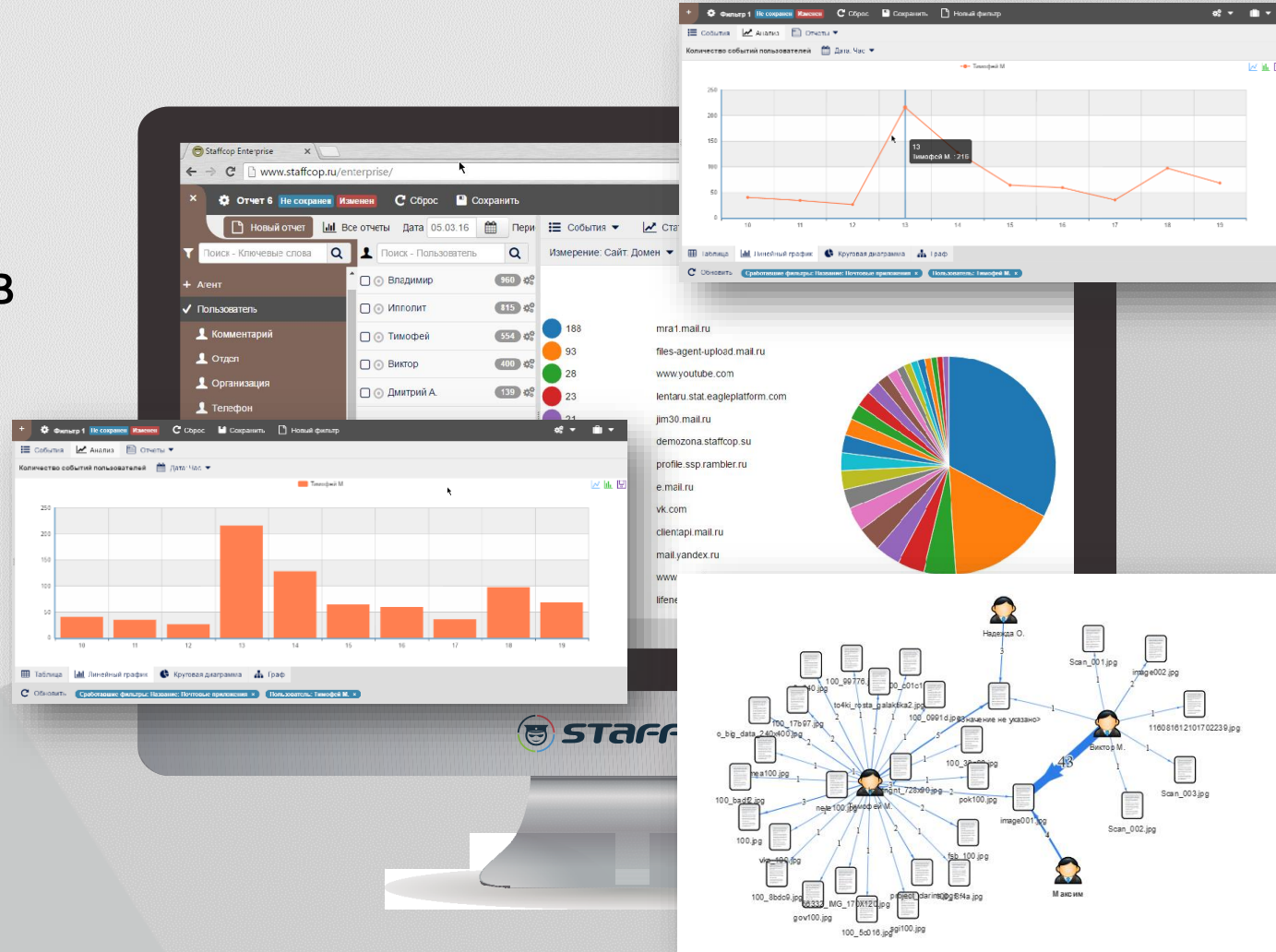
- контроль и блокировка

Теневое копирование файлов

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

Расследование инцидентов ИБ

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



Управление и администрирование



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

Аспекты внедрения



Правовые



Технические



Административные

Аспекты внедрения

- **№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).

Аспекты внедрения

- 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.

Политика лицензирования и стоимость

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		

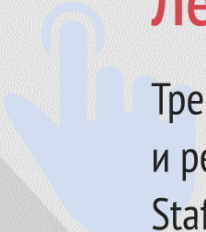
Тестируйте бесплатно до 3-х месяцев на парке машин любого размера.
Полнофункциональная версия. Техническое сопровождение проекта на всем протяжении.

Быстро



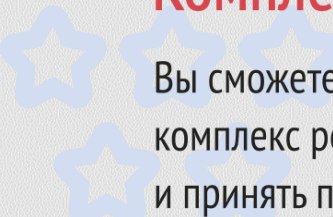
Развертывание пилотного проекта обычно занимает не более одного дня

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