Контроль над информационными потоками и действиями сотрудников.

Владимир Антонов
Аналитик информационной безопасности
ООО Атом Безопасность
v.antonov@staffcop.ru

STAFFCOP

- 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.

www.amtestlab.ru CERTIFIED AM TEST LAB REG # 00158 02/2016

Sk Сколково

академпарк Технопарк Новосибирского Академгородка

infosecurity RUSSIA

BIS SUMMIT 2018

Минкомсвязь России

Федеральная служба по техническому и экспортному контролю

STAFFCOP

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
-

ubuntu

PostgreSQL

- 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

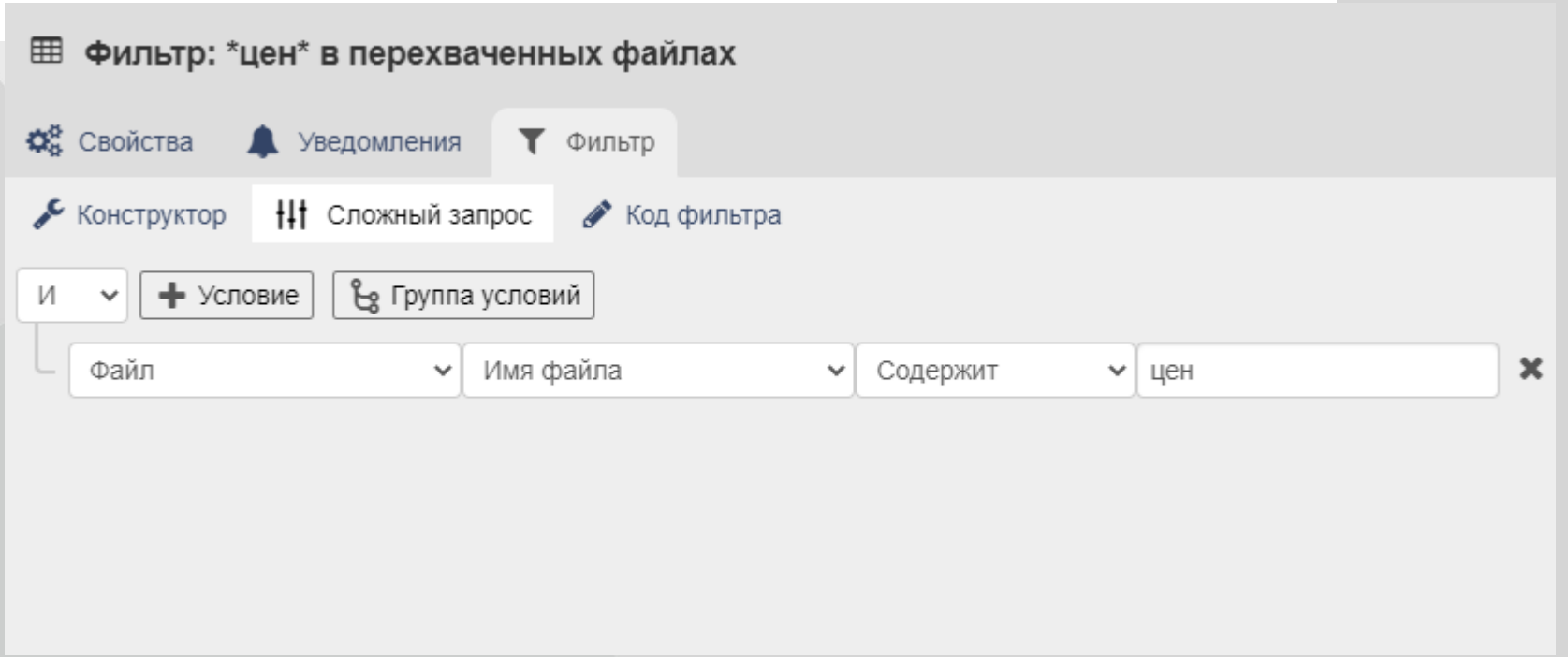
- Архив данных
- Конструктор многомерных отчетов
- Поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений
- Гибкая система настройки фильтров

Управление и администрирование

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

Теневые копии файлов – поиск по атрибутам

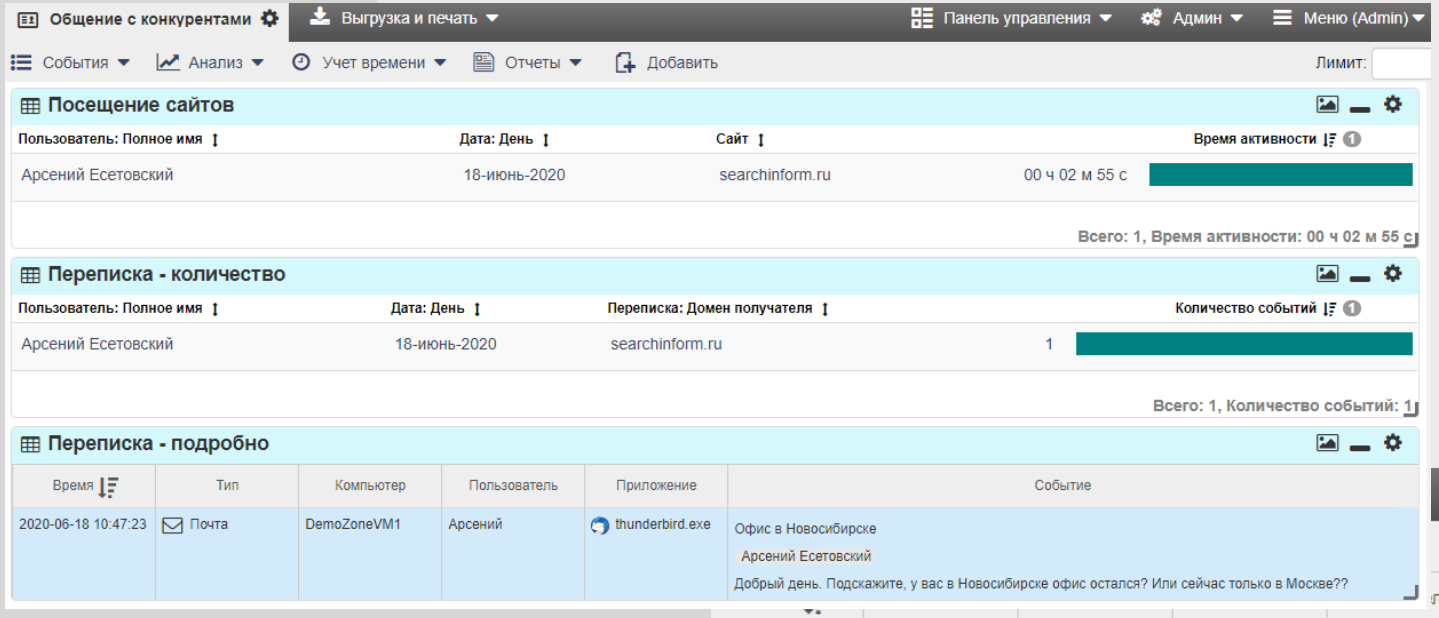
Время	Компьютер	Пользователь	Приложение	Контент	Связано с	Страниц	Размер	Получатели
2020-07-08 12:34	DemoZoneVM2	Ксения	explorer.exe	Скачать Входные цены.xlsx	FileOperation		8.2 Kb	
2020-06-14 17:25	DemoZoneNB4	BoDa		Скачать входные цены.xlsx	PrintDoc	1	8.2 Kb	
2020-06-14 16:47	DemoZoneNB3	d.borislavskiy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

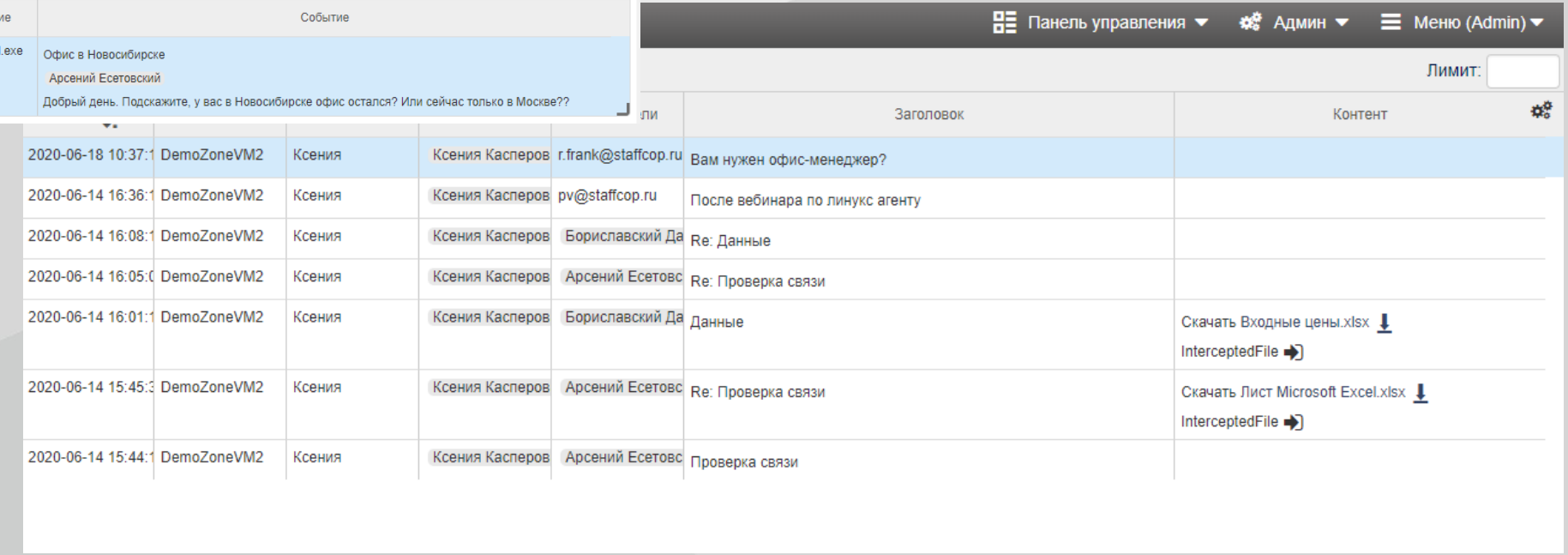


Теневые копии файлов – поиск по тексту

Перехваченный ф	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 ф	DemoZoneVM1	Арсений	thunderbird.exe	Ищем директора Картиночка.jpg  Скачать Картиночка.jpg Ксения Касперова Картина продиректора Mail

Общение с конкурентами и личная почта





Сканы паспортов и номера кредитных карт

Время 2020-11-17 11:48:15

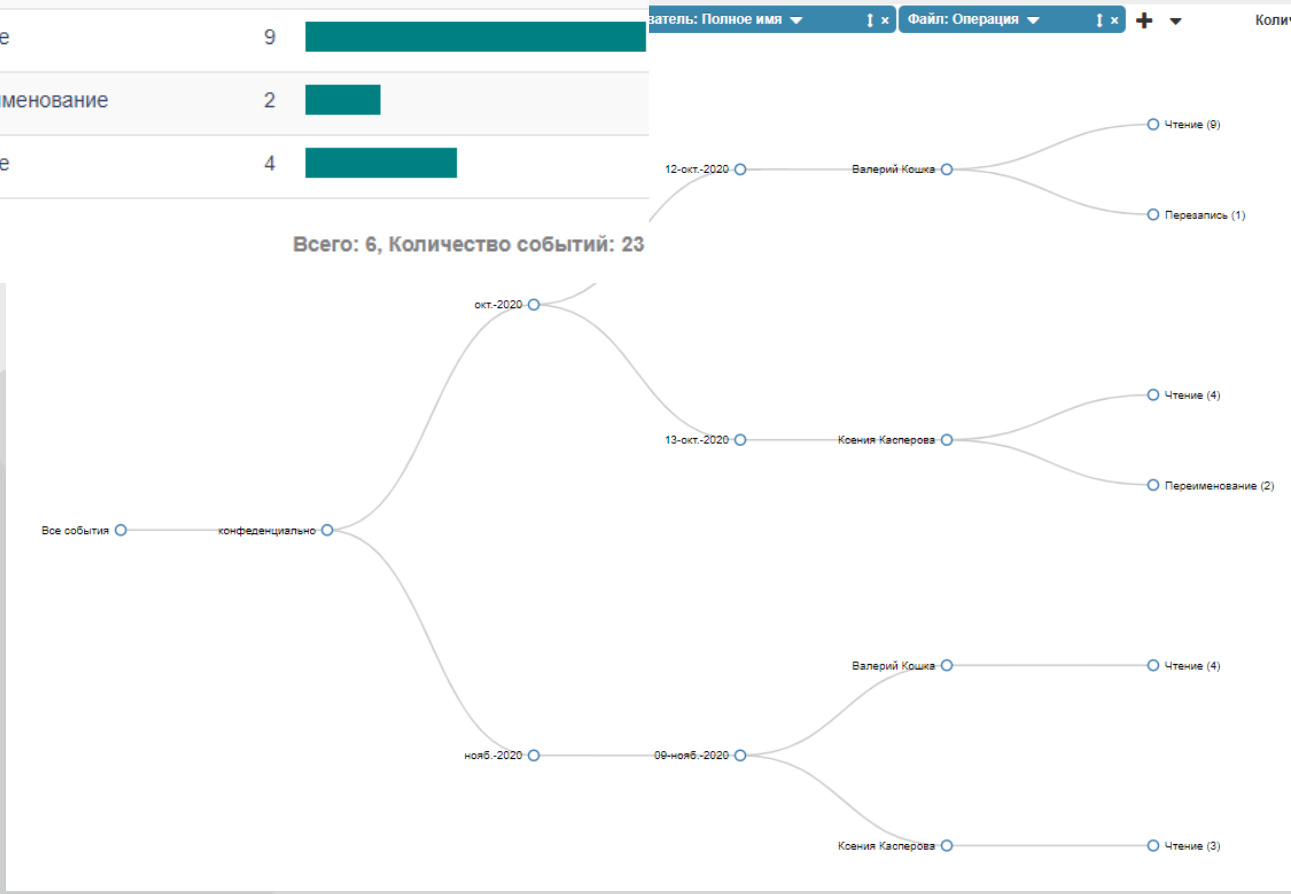
Фильтр Сервер распознаваний

Контент

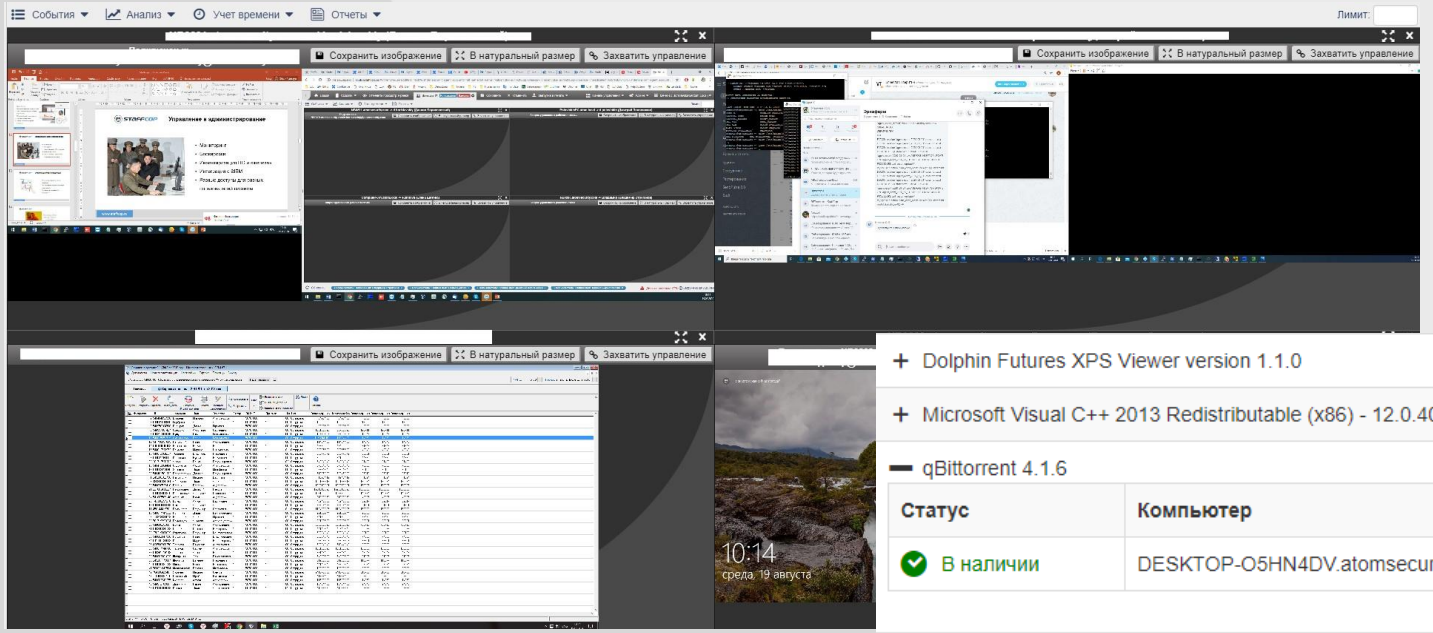
				Скачать Documents.7z
	DemoZoneVM2	Ксения	chrome.exe	Кредитные карты Ксения Касперова Сначала деньги, потом остальное 4276160971368577 сбер вс, 14 июн. 2020 г. в 16:06, Даниил Борославский <d.borislavskiy@staffcop.ru>: норм, давай ещё вс, 14 июн. 2020 г. в 16:01, Ксения Касперова <kkasperova522@gmail.com>: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

Метки на файлы

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



Управление и администрирование



+ Dolphin Futures XPS Viewer version 1.1.0
+ Microsoft Visual C++ 2013 Redistributable (x86) - 12.0.40649
− qBittorrent 4.1.6

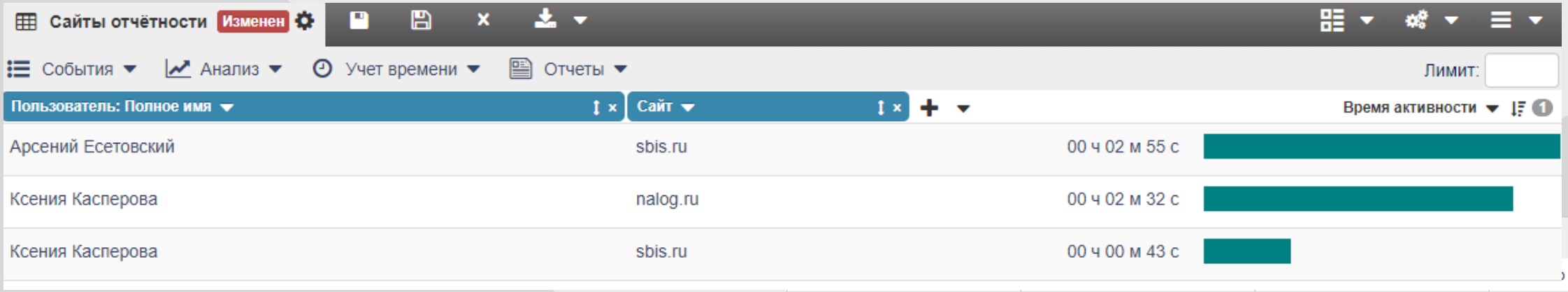
Статус	Компьютер	Поставщик	Версия	Дата наличия
В наличии	DESKTOP-O5HN4DV.atomsecurity.com	The qBittorrent project	4.1.6	17:06:25 04.06.2020

+ 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

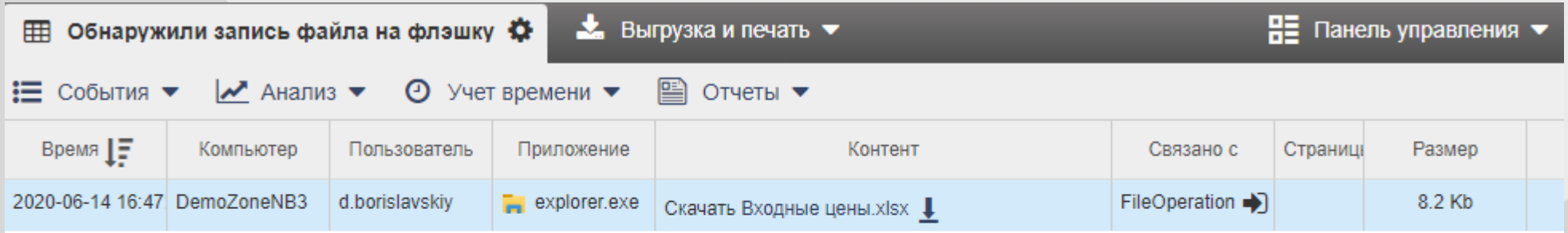
+ Обновление безопасности для Windows XP (KB2820917)
+ Обновление безопасности для Windows XP (KB976323)

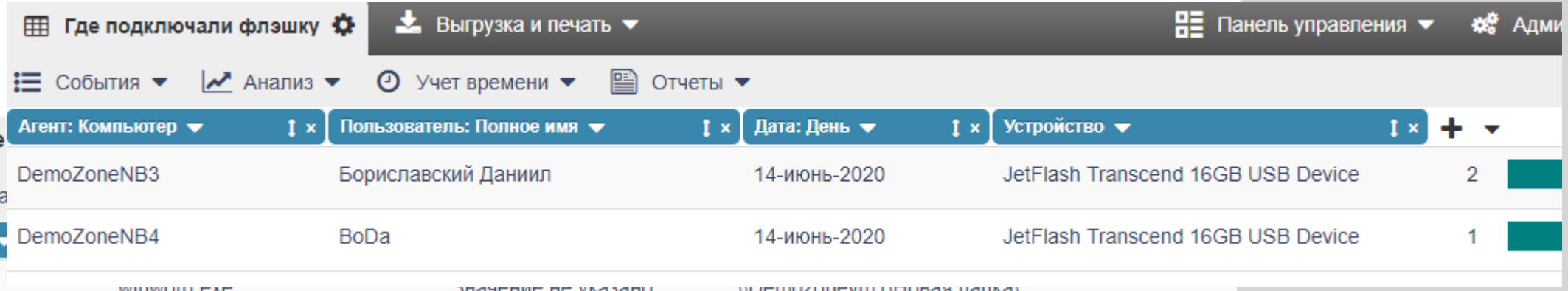
Поисковые запросы и посещение сайтов

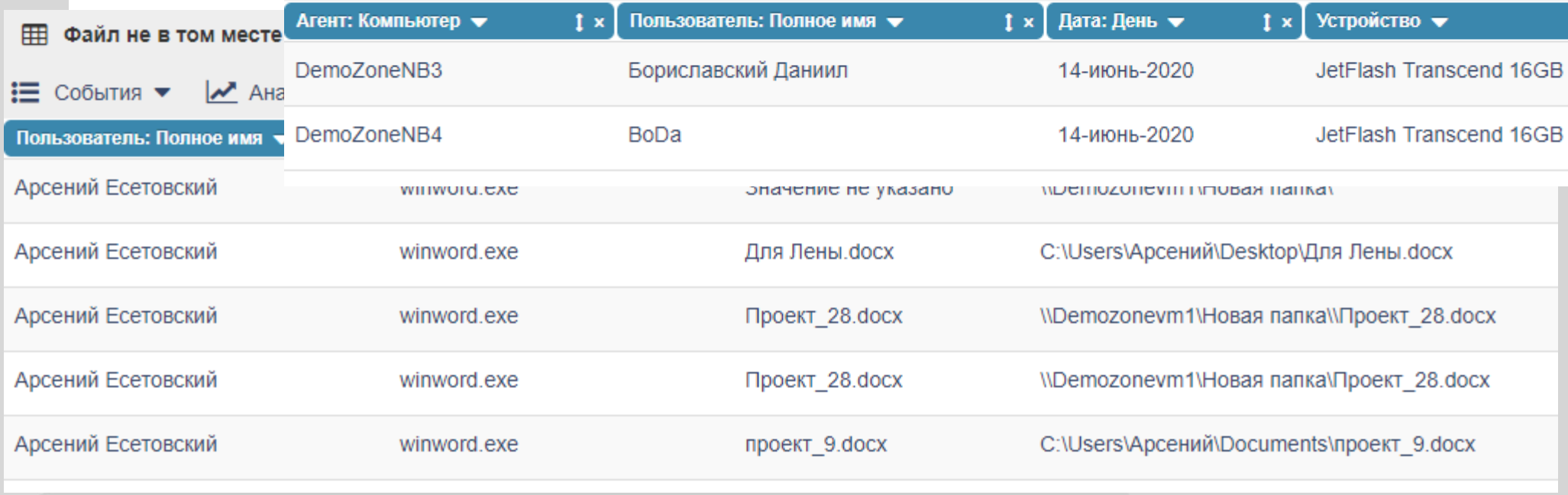


			Текст
			запада 3 сезон 5 серия
Арсений	firefox.exe	youtube.com	мир дикого запада 3 сезон
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	youtube
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	soliter.exe
Арсений	firefox.exe	yandex.ru	солитер виндовс 7 скачать 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

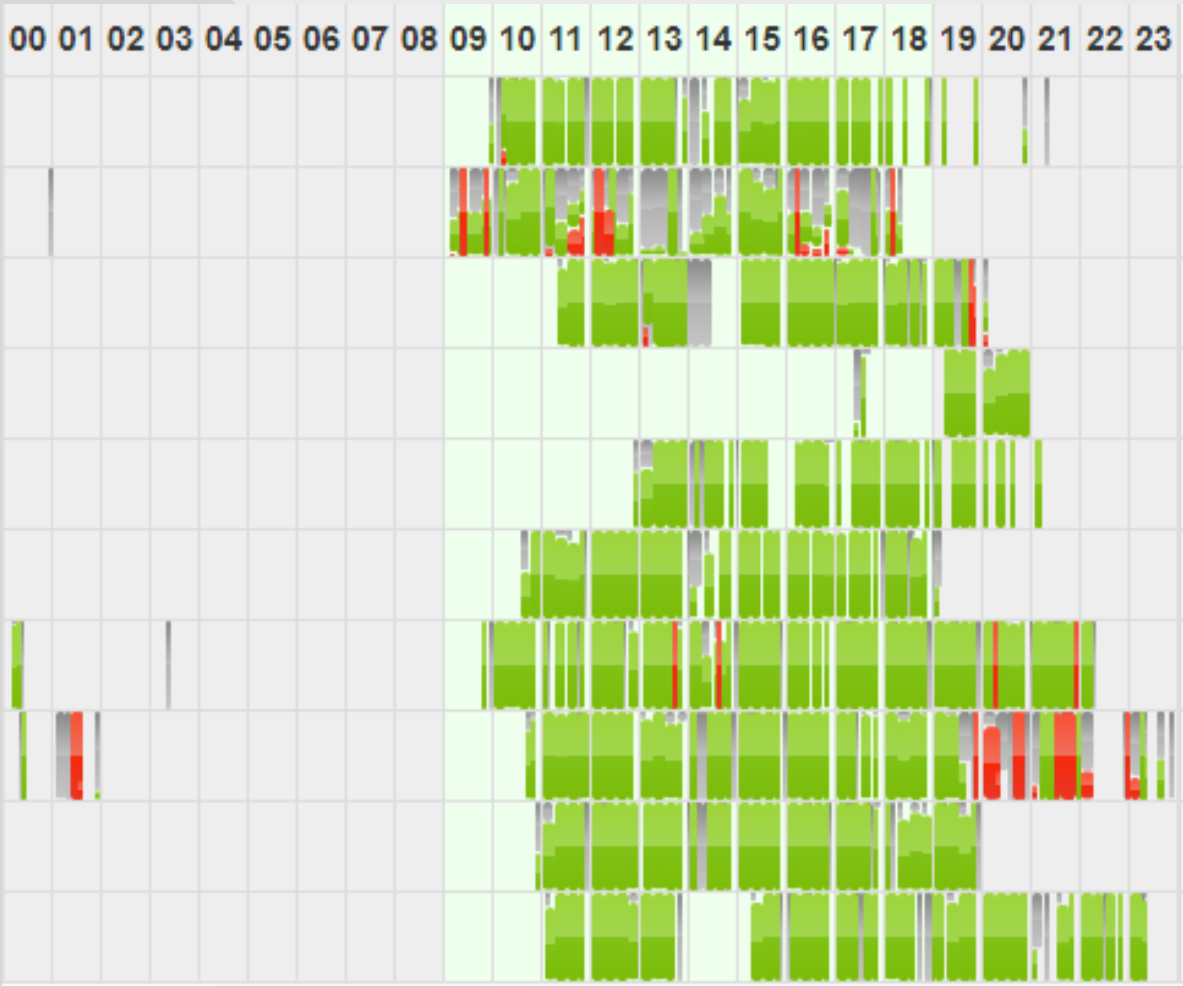
Расследование инцидентов







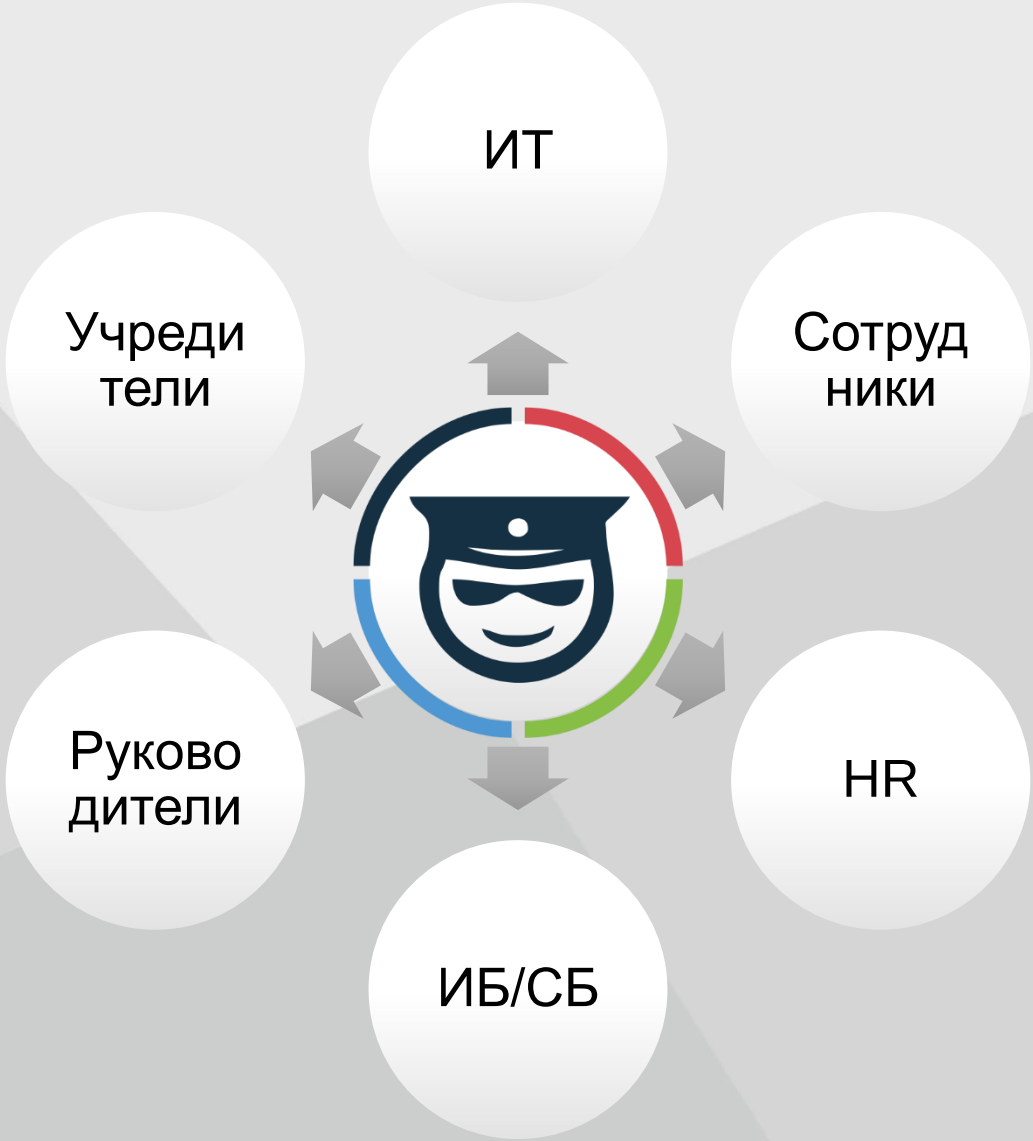
Учёт рабочего времени и его оценка



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

Потребители



Преимущества

На opensource решенияхи, не требует дополнительного платного ПО.

Цена.

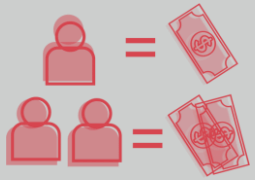
Входим в реестр отечественного ПО и имеет сертификат ФСТЭК.

Небольшие требования к железу для сервера.

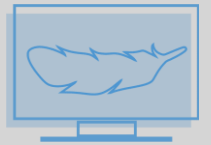
Настраиваемые отчёты и OLAP

Не мешает бизнесу работать.

Техническое сопровождение с начального этапа тестирования.



Единое решение и гибкая политика лицензирования.



Лёгкий агент.

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 ₽ / 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!

Владимир Антонов
Аналитик информационной безопасности
ООО Атом Безопасность

+7(499)6382809 доб. 236
v.antonov@staffcop.ru
v.antonov