



Система контроля для обеспечения комплекса мер защиты информационных и технологически процессов.

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



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



Своевременное обнаружение и предотвращение угроз ИБ и ЭБ
Организованное расследование инцидентов
Анализ деятельности сотрудников



Учет рабочего времени и оценка продуктивности сотрудников
Мониторинг бизнес-процессов и анализ эффективности сотрудников



Инвентаризация программного и аппаратного обеспечения
Удаленное администрирование машин пользователей

Задачи и цели контроля.

Зачем?

Надежность

Сложность
контроля

Как?

Оперативность

Точность

«Невмешательство»

Что?

Люди

Процессы

Технологии

Как устроен Staffcop:



Сервер использует базу данных PostgreSQL и работает на операционной системе ubuntu



Контроль ПК под управлением различных OS:

Windows, Linux, MacOS

Множество способов установки агентов, как локальные, так и удаленные.


Для организации сервера достаточно одной виртуальной машины и система готова к сбору сразу после установки

Инвентаризация «железа» и ПО


Сканирование хранящихся файлов

Снимки с веб-камер


Скриншоты и запись видео рабочего стола


 Мониторинг посещенных сайтов и поисковых запросов


 Подключение к рабочему столу

 Мониторинг действий в социальных сетях

 Контроль печати

 Контроль email-переписки

 Перехват сообщений в мессенджерах

 Контроль USB и CD

 Кейлоггер

 Мониторинг доступа к файлам

 Запись аудио с микрофона и колонок



Копия файла на сервере

- Электронная почта
- Съёмные носители
- Передача через интернет
- Печать на принтере

USB-порты

- Контроль подключений
- Операции с файлами
- Блокировка накопителей
- Черные и белые списки

Интернет-мессенджер

- Skype
- ICQ, QIP, Jabber(XMPP)
- Mail.ru, Yahoo
- Telegram

Передача гипертекстовой информации и файлов

- HTTP/HTTPS
- FTP/FTPS
- POST и GET запросы

Почтовые протоколы

- SMTP/SMTSPS
- IMAP
- POP3/POP3S
- MAPI (MS Exchange)

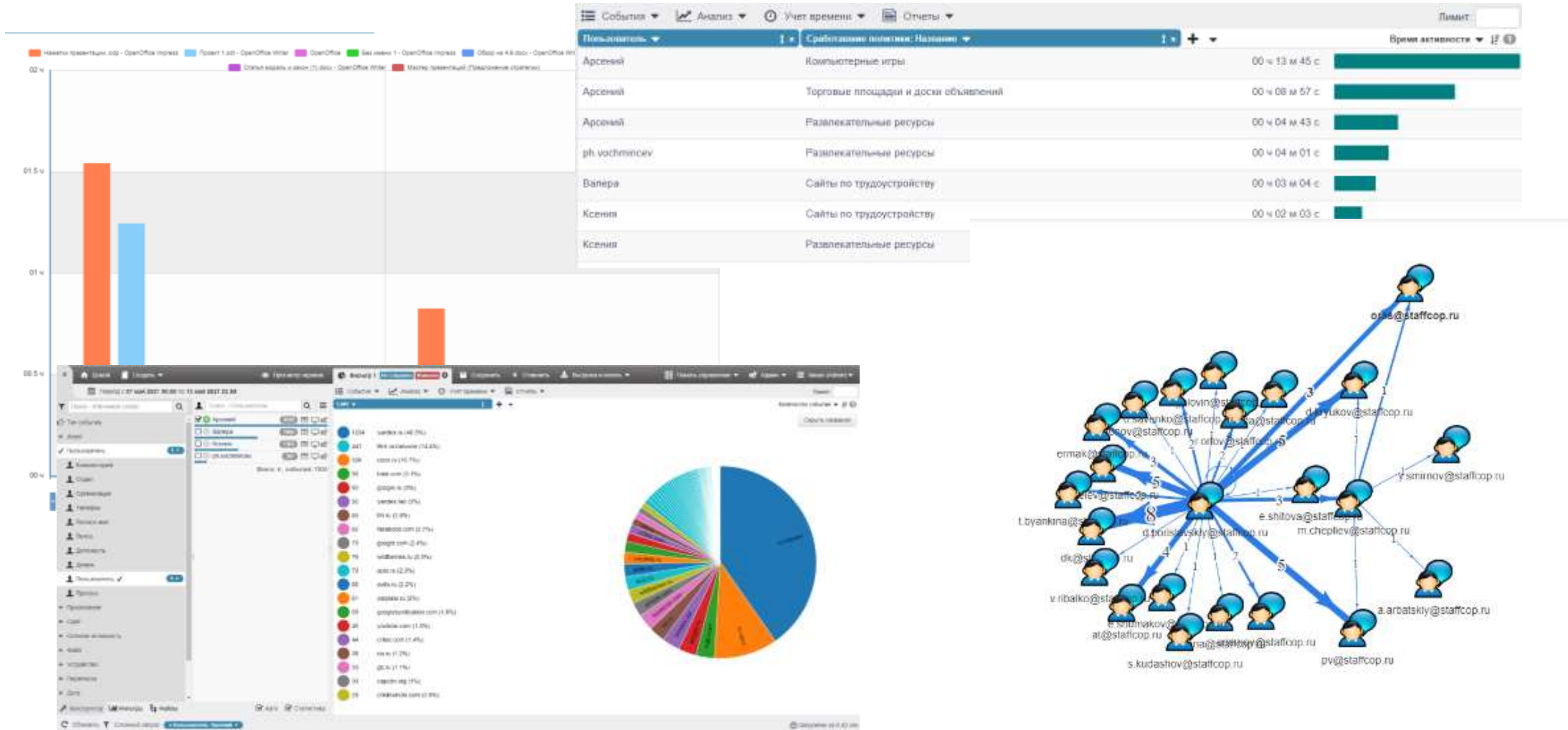
Декодирование сервисов веб-почты и соц.сетей

- Mail.ru, Yandex.ru, gmail.com и т.п.
- VK, FB, Одноклассники и т.п.

- Долгосрочный архив событий
- Конструктор многомерных отчетов
- Создание словарей и поиск по словам и регулярным выражениям
- Множество графов и диаграмм
- Система оповещений по инцидентам
- Гибкая система фильтрации информации



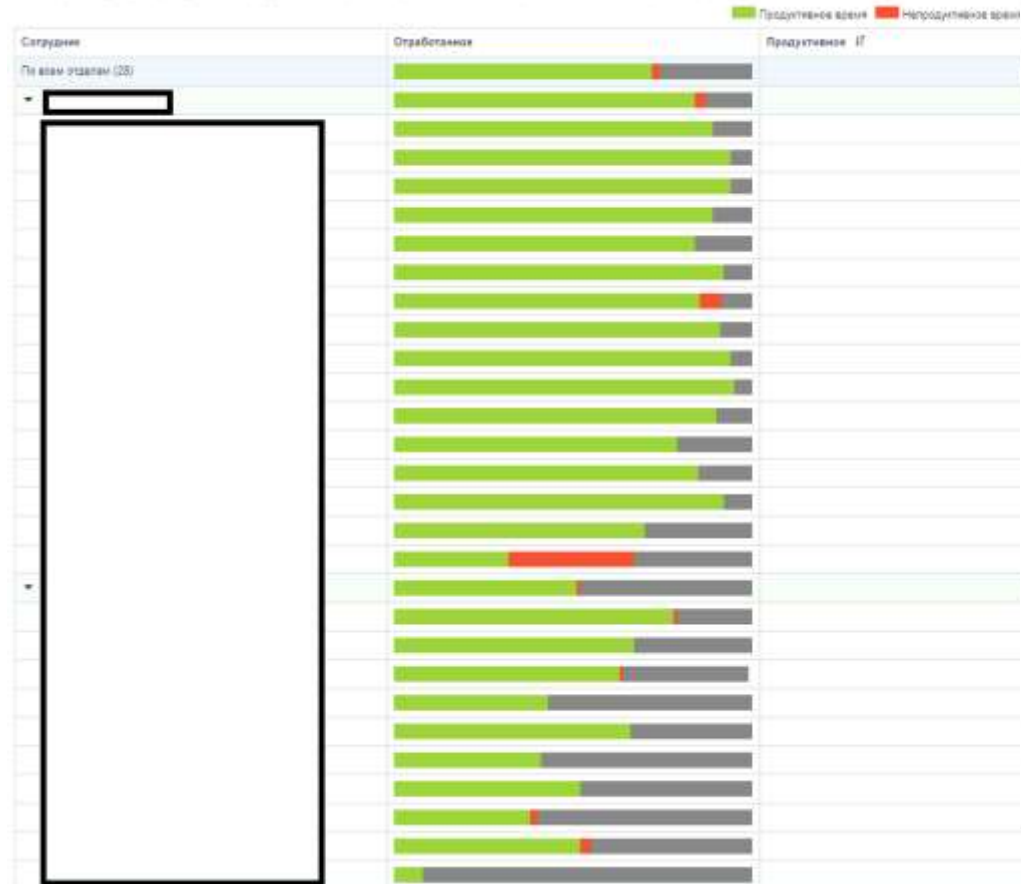
Точность – анализ и формирование конкретных задач



Люди – один из наиболее ценных ресурсов.

Продуктивное время за период с 31 мая 2021 по 31 мая 2021

Счёт отражает суммарное продуктивное/непродуктивное и нейтральное время пользователей на рабочих местах за выбранный период времени от общей активности пользователя.



Учёт рабочего времени за период с 19 мая 2021 по 19 мая 2021

19 мая 2021 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 При

Чеплиев Максим Валерьевич

Чеплиев Максим Валерьевич 11:51:32 20:50:00 8:58:28 8:29:29 0:

Продуктивность

Категория	Время	Процент
Всё остальное	3:15:15	38.32%
Приложения для удалённого доступа	1:12:09	14.16%
Офисные приложения	1:10:36	13.86%
Корпоративные ресурсы	1:01:58	12.16%
Поисковые порталы	0:53:44	10.55%
PDF IEXPLORE	0:16:12	3.18%
Корп ресурсы	0:09:19	1.83%
Интернет-мессенджеры	0:09:00	1.77%
Информационная безопасность	0:08:47	1.72%
Блокировка экрана, заставка	0:04:16	0.84%
Приложения для SIP-телефонии	0:03:43	0.73%
Активация Windows	0:02:57	0.35%
Итого	8:29:29	100.00%

Мониторинг

Блокировки

Инвентаризация ПО и «железа»

Уровни доступа к данным и функционалу в системе

Интеграция с SIEM


Процесс внедрения, создание точек контроля, уведомлений и организация.

В основной интерфейс Инциденты
Фильтр + Новый инцидент

	Инциденты	ID ↓	Дата	Тема	Группа	Статус	Создал	Назначен	Приоритет	Шаблон реагирования	Фильтр
	Статусы	13	01.06.2021 13:17	На основании фильтра 1010 "Поиск по словарю 3"	Утечка данных		Admin User	Maxim Chepliev	Незначительный	Найти утечку	Конфиденциальная информация
	Группы инцидентов	12	01.06.2021 13:07	На основании фильтра 1010 "Поиск по словарю 3"	Утечка данных		Admin User	Maxim Chepliev	Незначительный	Найти утечку	Конфиденциальная информация
	Шаблоны реагирования	11	26.05.2021	На основании фильтра	Утечка данных		Admin User	Maxim	Незначительный	Ограничить доступ к данным и каналам	Фильтр 1
	Сводные отчеты										
	Недоменная отправка файлов										
	Перепишка: Отправитель ↓										
	kkasperova522@gmail.com	5		тра	Утечка данных		Admin User				
	arseniiset@ngs.ru	4		тра	Наличие недопустимой информации		Admin User				
	Отправка на флешку										
	Пользователь: Полное имя ↓										
	Устройство: ID устройства ↓										
	Нет данных за период, попадающих под фильтр										

Фильтр 1

- 39 Конфиденциальная информация (18.7%)
- 27 Пароль в браузере (12.9%)
- 20 Развлекательные ресурсы (9.6%)
- 18 Торговые площадки и доски объявлений (8.6%)



Поиск по словарю: Конфиденциальная информация

⚙️ Свойства
🔔 Уведомления
⏴ Фильтр

Активировать уведомления

Регулярность:

- Новые
- Ежедневно
- Еженедельно
- Ежемесячно 1 ↓ числа

Время отправки:

Создать инцидент

Шаблон реагирования:

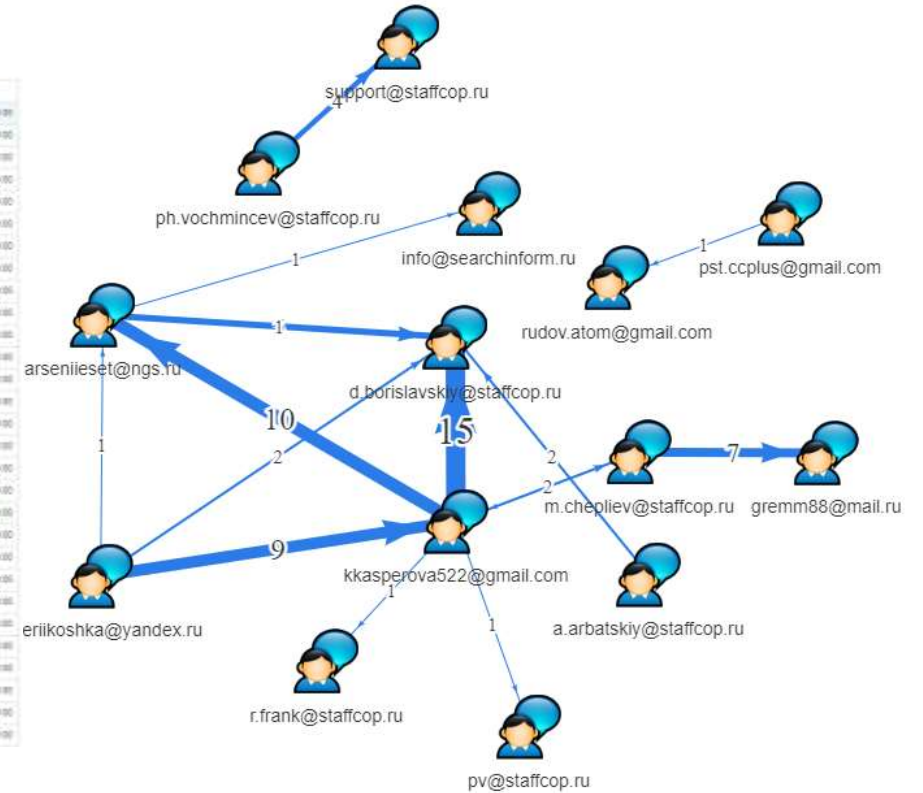
Группа инцидента:

Кому:

Активное время за период с 31 мая 2021 по 31 мая 2021

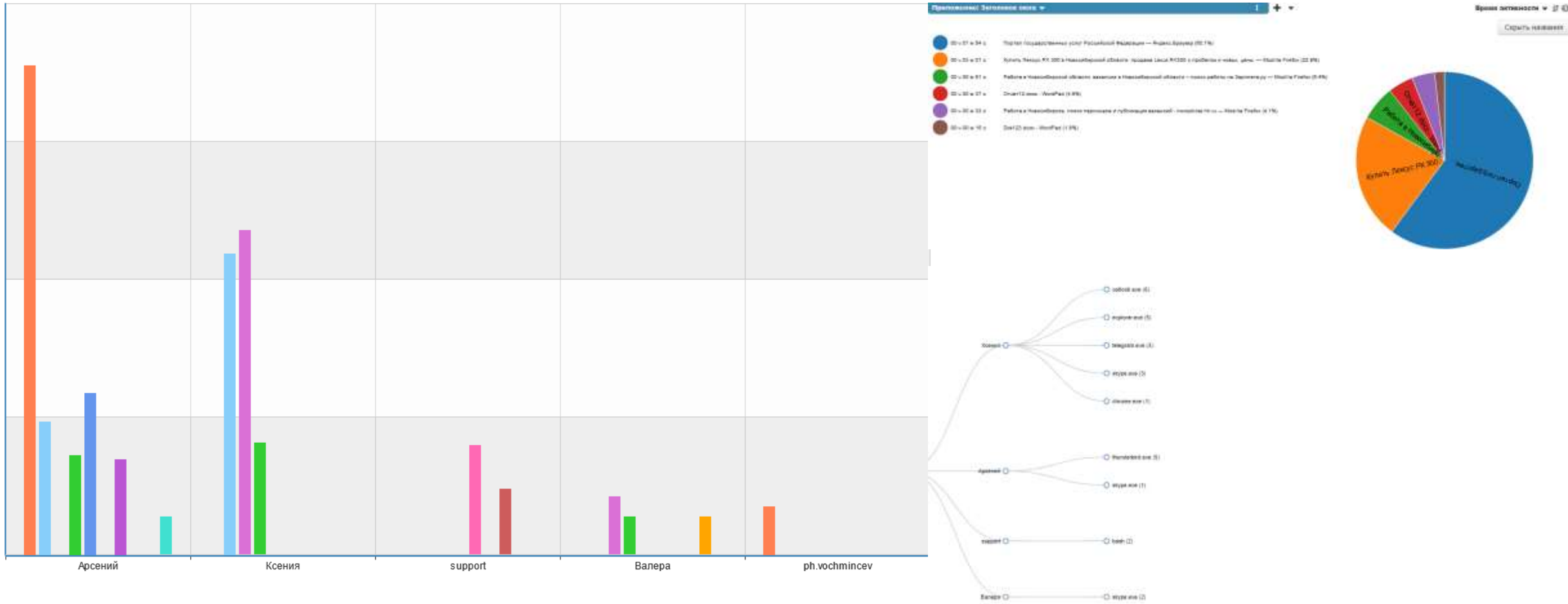
Отчет отражает суммарное активное и неактивное время пользователей за выбранный период времени по отчислениям и переводам.

Состояние	Описание	Активное	Неактивное	Переводы	Направление	Ссылка	Платежи
По всем адресам (23)		178,04:00 (89,02 %)			10,20:00 (5,14 %)		188,24:00
Абонентский (16)		188,23:12 (94,1 %)			8,08:48 (4,0 %)		196,32:00
		8:10:00 (4,0 %)	1:10:00 (0,5 %)				9:20:00
		7:44:00 (4,2 %)	0:44:00 (0,2 %)				8:28:00
		7:20:00 (4,0 %)	0:20:00 (0,1 %)				7:40:00
		7:10:00 (4,0 %)	0:10:00 (0,0 %)				7:20:00
		7:11:00 (4,0 %)	0:11:00 (0,0 %)				7:22:00
		7:01:00 (4,0 %)	0:01:00 (0,0 %)				7:02:00
		8:47:00 (4,7 %)			0:10:00 (0,0 %)		9:57:00
		8:49:44 (4,8 %)			0:11:16 (0,0 %)		10:01:00
		8:39:49 (4,7 %)			0:09:18 (0,0 %)		9:49:07
		8:28:19 (4,6 %)			0:09:01 (0,0 %)		9:37:20
		8:25:19 (4,6 %)			0:08:39 (0,0 %)		9:33:58
		8:08:00 (4,5 %)			0:07:07 (0,0 %)		9:15:07
		8:02:18 (4,5 %)			1:07:49 (0,5 %)		9:10:07
		4:48:17 (2,5 %)			0:18:40 (0,0 %)		5:06:57
		3:49:01 (2,0 %)			0:13:39 (0,0 %)		4:02:40
Телефонная Поддержка (7)		94:26:28 (46,3 %)			4:52:59 (2,5 %)		99:19:27
		8:03:01 (4,0 %)	2:02:01 (1,0 %)				10:05:02
		8:20:46 (4,6 %)	1:18:46 (0,6 %)				9:39:32
		7:30:00 (4,1 %)	0:38:58 (0,2 %)				8:08:58
		7:07:47 (3,9 %)	0:27:47 (0,1 %)				7:35:34
		7:04:16 (3,9 %)	0:04:16 (0,0 %)				7:08:32
		8:13:09 (4,5 %)			0:48:01 (0,2 %)		9:01:10
		8:06:04 (4,5 %)			0:08:00 (0,0 %)		8:14:04
		8:16:40 (4,6 %)			1:28:33 (0,6 %)		9:45:13
		8:06:07 (4,5 %)			0:01:58 (0,0 %)		8:08:05
		7:48:48 (4,2 %)			4:44:14 (2,3 %)		12:33:02



Человек и процессы

■ firefox.exe
 ■ msedge.exe
 ■ chrome.exe
 ■ explorer.exe
 ■ telegram.exe
 ■ bash
 ■ skype.exe
 ■ shell
 ■ browser.exe
 ■ lockapp.exe



2021-06-21 12:51:22	enterprise	Удаление приложения	libnginx-mod-http-xslt-filter
2021-06-21 12:51:22	enterprise	Удаление приложения	ufw
2021-06-21 12:51:22	enterprise	Удаление приложения	isc-dhcp-common
2021-06-21 12:51:22	enterprise	Удаление приложения	install-info
2021-06-21 12:51:22	enterprise	Удаление приложения	apport
2021-06-21 12:51:22	enterprise	Установка приложения	liblz4-1:amd64
2021-06-21 12:51:22	enterprise	Удаление приложения	nginx-common

Инвентаризация - Устройства

Статус ↑	Компьютер ↑	Производитель ↑	Тип устройства ↑	HWID ↑	Дата наличия ↑
➔ Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IKEv2)	SWD\MSRRAS\MS_AGILEVPNMI	17:50:00 09.07.2021
➔ Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IPv6)	SWD\MSRRAS\MS_NDISWANIPV	17:50:00 09.07.2021
➔ Добавлено	Arsenii	GenuineIntel	CPU: Intel(R) Xeon(R) CPU E5-2470 v2 @ 2.40GHz	CPU0	17:50:00 09.07.2021
➔ Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (Network Monitor)	SWD\MSRRAS\MS_NDISWANBH	17:50:00 09.07.2021
➔ Добавлено	Arsenii		Printer: Fax		17:50:00 09.07.2021
➔ Добавлено	Arsenii	(Standard system devices)	Mouse: USB Input Device	USB\VID_0E0F&PID_0003&MI_0	17:50:00 09.07.2021
➔ Добавлено	Arsenii	Microsoft	Mouse: PS/2 Compatible Mouse	ACPI\VMW0003\4&1BD7F811&0	17:50:00 09.07.2021
➔ Добавлено	Arsenii	Microsoft	Network Adapter: WAN Miniport (IP)	SWD\MSRRAS\MS_NDISWANIP	17:50:00 09.07.2021
➔ Добавлено	Arsenii	(Standard disk drives)	Disk Drive: VMware Virtual disk SCSI Disk Device	SCSI\DISK&VEN_VMWARE&PRC	17:50:00 09.07.2021

Процессы и технологии



СИСТЕМА	Процесс	Число
СИСТЕМА	Удаление	25
Ксения	Создание	15
Арсений	Копирование	14
Ксения	Копирование	12
Арсений	Создание	8
Валера	Перезапись	8
Ксения	Удаление	5
Ксения	Подключение	4
Ксения	Запись	3
Ксения	Переименование	3
Валера	Создание	3
Валера	Переименование	3
Арсений	Запись	3
Валера	Копирование	2
Арсений	Переименование	2
Ксения	Перемещение	1
Валера	Подключение	1
Валера	Запись	1

Почему мы?



Многомерные аналитические отчеты, схемы коммуникаций и движения информации с возможностью перехода от общего к частному



Мониторинг и анализ событий на рабочих местах из единого веб-интерфейса, возможность просто и безопасно организовать доступ к серверу



Работа в любых сетевых инфраструктурах – подойдет для контроля распределенной филиальной сети, удаленных офисов и сотрудников



Подробная документация, оперативная и компетентная техническая поддержка. Команда проекта обеспечивает полноценное сопровождение с начального этапа тестирования



Возможность доработки под требования заказчика, в том числе, интеграции с другими системами и бизнес-процессам заказчика



Staffcop подходит для выполнения требований банковских ГОСТов, приказов ФСТЭК России и для работы на объектах КИИ



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!

Чеплиёв Максим
Специалист отдела аналитики
ООО Атом Безопасность

 +7(499)6382809 доб. 238
 m.chepliev@staffcop.ru