Расследование инцидентов ИБ и контроль работы сотрудников

Николай Сухотерин

Специалист по внедрению

ООО «АТОМ БЕЗОПАСНОСТЬ»

staffcop®

Расследование инцидентов внутренней безопасности

О компании

Единая консоль и многомерная архитектура данных позволяют расследовать любой инцидент за несколько кликов

10+лет

Разработки приложений контроля сотрудников

Импортонезависмый продукт. Российский разработчик

ФСТЭК России
Федеральная служба по техническому и экспортному контролю

4 уровень доверия

100+

Сотрудников

200

Конференций, в которых мы приняли участие за 3 года

Контур

В группе компаний

АРПП Отечественный софт

Минцифры России

Sk Участник

академпарк

staffcop®

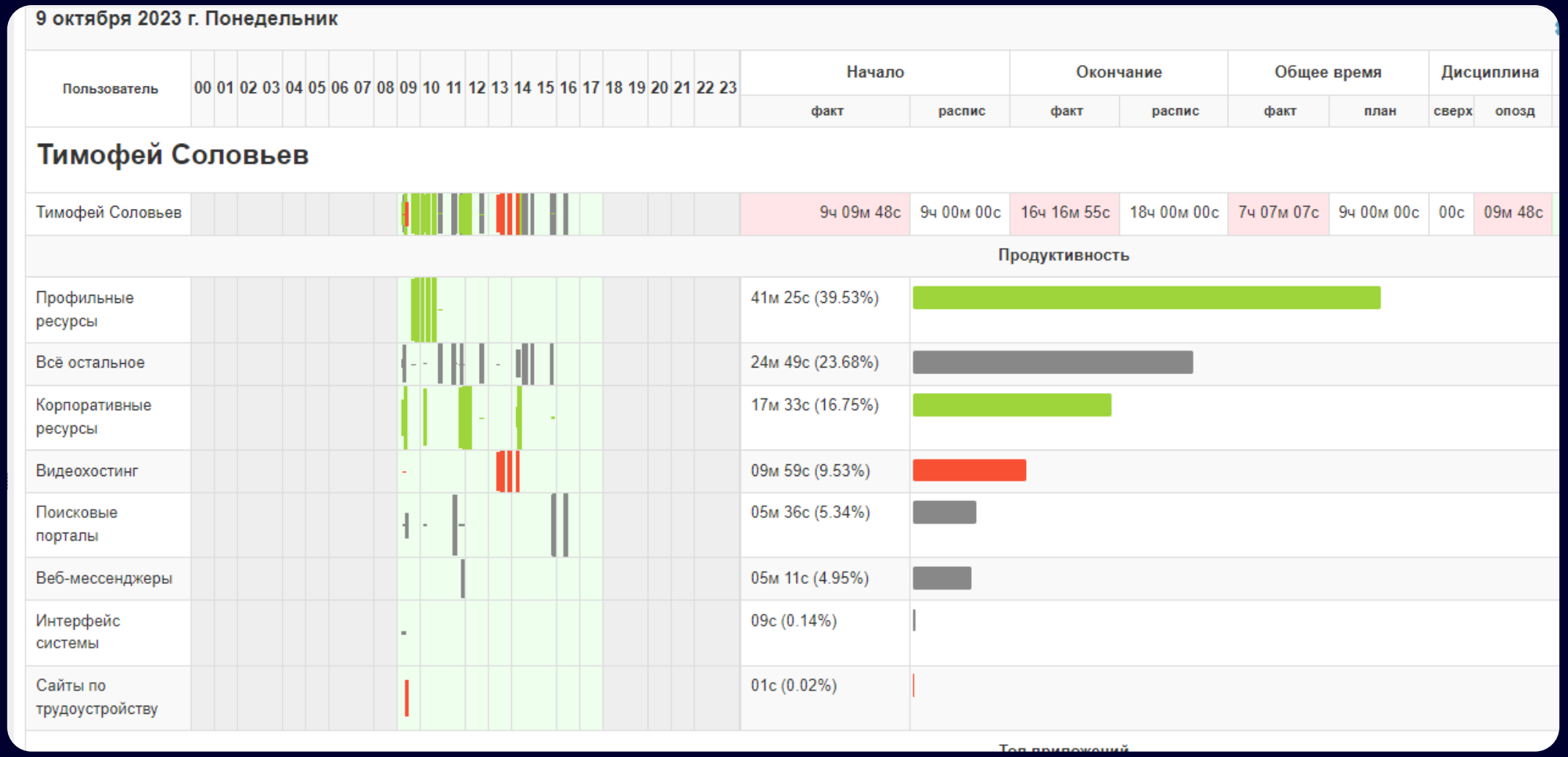
О чем поговорим в ближайшие двадцать минут:

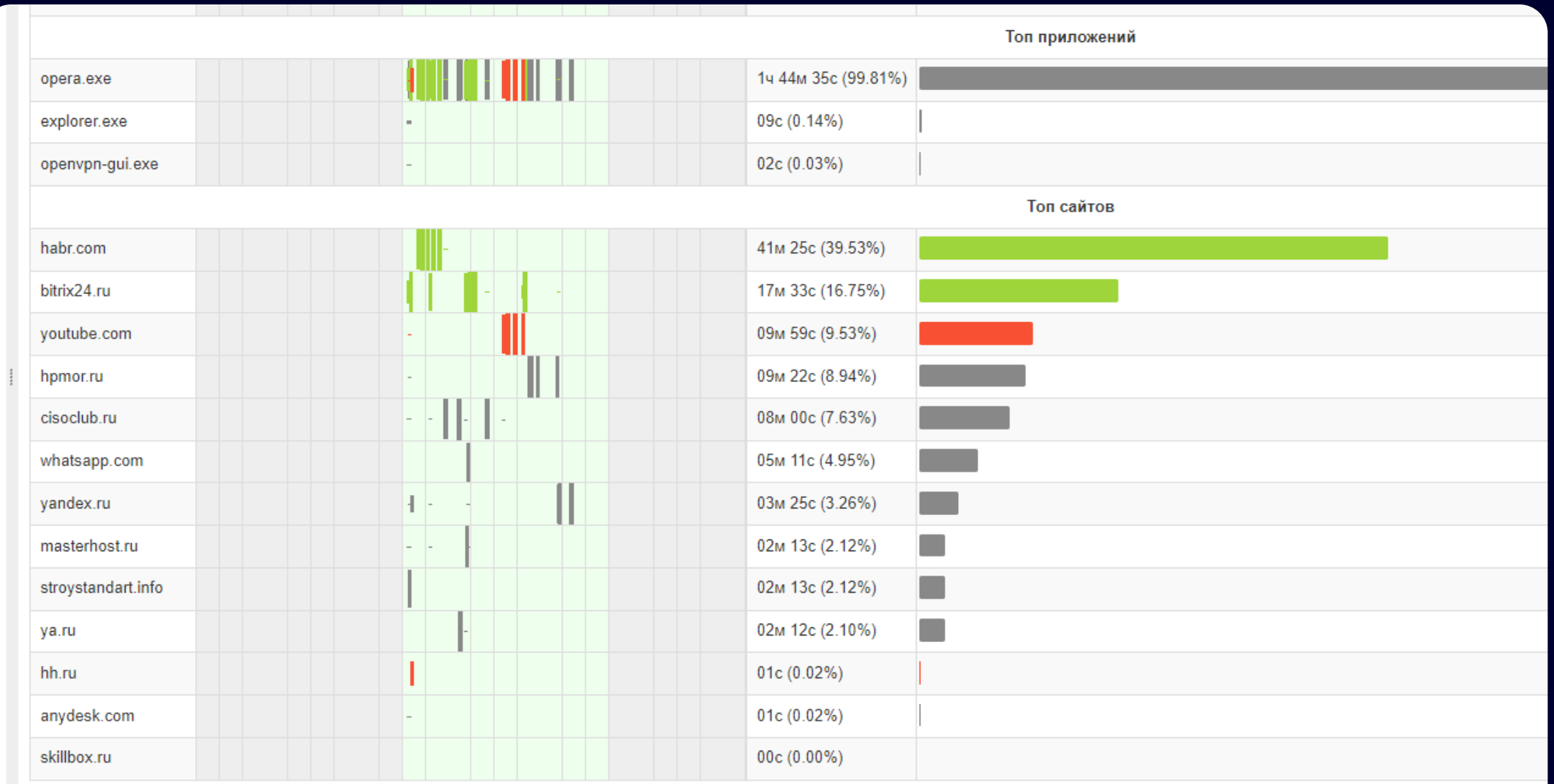
- Организация бизнес-процессов
- Махинации сотрудников и их личные интересы
- Требования законодательства по отношению к компаниям

Как наше решение помогает разбираться с этими проблемами

staffcop

Организация бизнес процессов



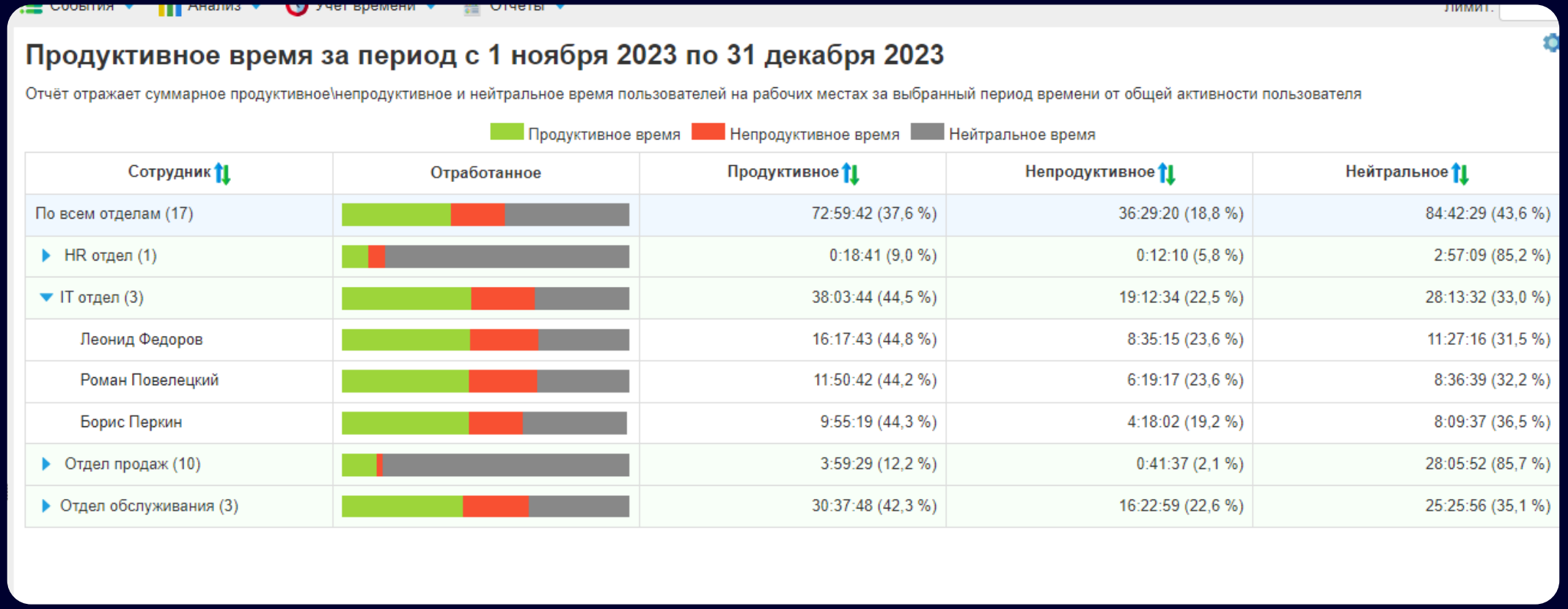


Топ приложений

opera.exe	1ч 44м 35с (99.81%)
explorer.exe	09с (0.14%)
openvpn-gui.exe	02с (0.03%)

Топ сайтов

habr.com	41м 25с (39.53%)
bitrix24.ru	17м 33с (16.75%)
youtube.com	09м 59с (9.53%)
hpmor.ru	09м 22с (8.94%)
cisoclub.ru	08м 00с (7.63%)
whatsapp.com	05м 11с (4.95%)
yandex.ru	03м 25с (3.26%)
masterhost.ru	02м 13с (2.12%)
stroystandart.info	02м 13с (2.12%)
ya.ru	02м 12с (2.10%)
hh.ru	01с (0.02%)
anydesk.com	01с (0.02%)
skillbox.ru	00с (0.00%)



Продуктивное время за период с 1 ноября 2023 по 31 декабря 2023

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 (17)		72:59:42 (37,6 %)	36:29:20 (18,8 %)	84:42:29 (43,6 %)
▶ HR отдел (1)		0:18:41 (9,0 %)	0:12:10 (5,8 %)	2:57:09 (85,2 %)
▼ IT отдел (3)		38:03:44 (44,5 %)	19:12:34 (22,5 %)	28:13:32 (33,0 %)
Леонид Федоров		16:17:43 (44,8 %)	8:35:15 (23,6 %)	11:27:16 (31,5 %)
Роман Повелецкий		11:50:42 (44,2 %)	6:19:17 (23,6 %)	8:36:39 (32,2 %)
Борис Перкин		9:55:19 (44,3 %)	4:18:02 (19,2 %)	8:09:37 (36,5 %)
▶ Отдел продаж (10)		3:59:29 (12,2 %)	0:41:37 (2,1 %)	28:05:52 (85,7 %)
▶ Отдел обслуживания (3)		30:37:48 (42,3 %)	16:22:59 (22,6 %)	25:25:56 (35,1 %)

staffcop

Топ опоздавших	Кол-во
Ксения Андреевна	144
Пользователь с Мака	9
Nikolay Macov	5
Артемий Дефендеров	5
Леонардо	4
Alexey	4
RedOS User	4
Микеланджело	4
Display Manager daemon	3
admin	3

Топ по времени опозданий	Кол-во
Ксения Андреевна	661:50:29
Пользователь с Мака	39:09:55
Nikolay Macov	22:46:36
Артемий Дефендеров	18:27:54
Display Manager daemon	15:45:37
RedOS User	15:03:43
admin	13:52:52
Alexey	12:20:11
Леонардо	10:28:41
Микеланджело	10:13:22

Топ активных	Кол-во
Микеланджело	41:23:06
Леонардо	37:43:06
Донателло	31:26:13
Ксения Андреевна	28:20:58
Рафаэль	26:54:35
Балдессаре Перуцци	22:41:36
Пользователь с Мака	2:36:53
RedOS User	1:57:34
Nikolay Macov	1:40:11
Артемий Дефендеров	1:11:46

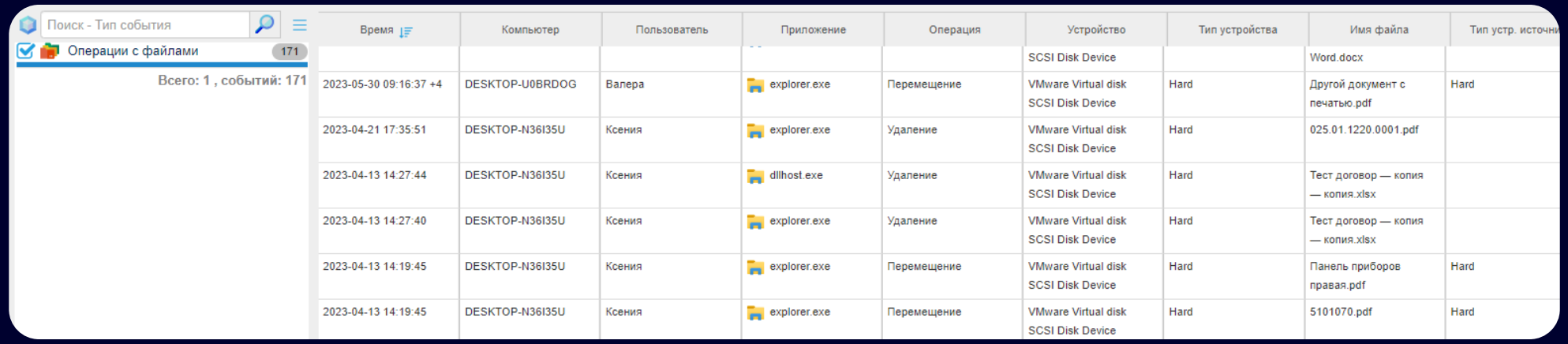
Топ неактивных	Кол-во
Ксения Андреевна	195:16:59
Пользователь с Мака	16:07:40
Балдессаре Перуцци	12:29:35
RedOS User	11:18:52
Артемий Дефендеров	6:06:09
Alexey	5:20:30
Донателло	4:39:25
Nikolay Macov	4:37:33
Леонардо	3:46:20
admin	1:37:17

Топ продуктивных	Кол-во
Микеланджело	17:13:47
Леонардо	16:20:38
Донателло	13:20:28
Рафаэль	11:52:09
Балдессаре Перуцци	9:56:35
Ксения Андреевна	3:54:42

Топ непродуктивных	Кол-во
Донателло	9:43:10
Леонардо	8:37:43
Микеланджело	6:41:33
Рафаэль	6:21:42
Балдессаре Перуцци	4:19:59
Ксения Андреевна	0:48:29

Махинации

Время	Тип	Компьютер	Пользователь	Приложение	Событие
2023-11-15 10:46:51	Интернет-пейджер	nb-asus-287	пк	browser.exe	Эфир.zip Скачать Эфир.zip Im
2023-11-07 09:12:46	Интернет-пейджер	nb-asus-287	пк	browser.exe	TRIAL_01_12_2023_025.zip Скачать TRIAL_01_12_2023_025.zip Im
2023-11-07 06:43:59	Почта	nb-asus-287	пк	outlook.exe	press@staffcop.ru Подключайтесь 8 ноября в 11:00 по МСК! Второй вебинар по свежему релизу 5.3 Словарь экстремистских выражений OriginalMessage_2023_11_07__09_12_37_A8.msg Скачать OriginalMessage_2023_11_07__09_12_37_A8.msg Mail
2023-11-03 17:11:59	Почта	nb-asus-287	пк	outlook.exe	d.semenova@spbtech.ru Отпуск делопроизводителя Уважаемые коллеги! Обращаю ваше внимание на то, что с 07.11.2023 по 10.11.2023 буду находиться в отпуске. На время моего отсутс

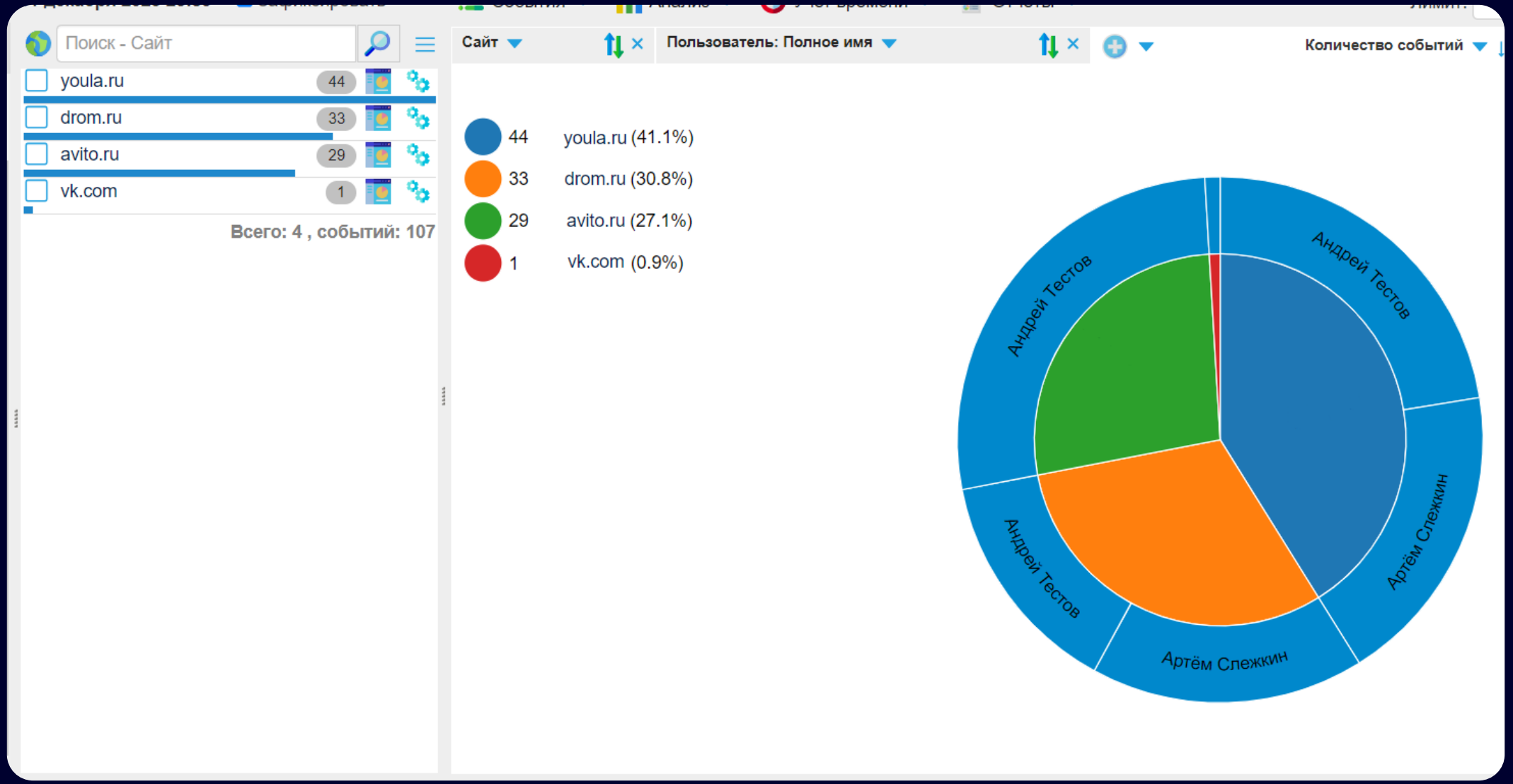


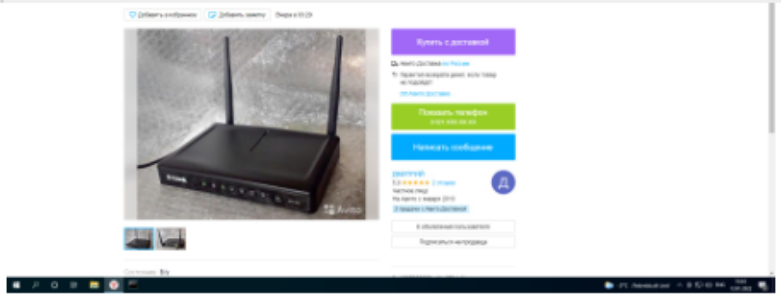
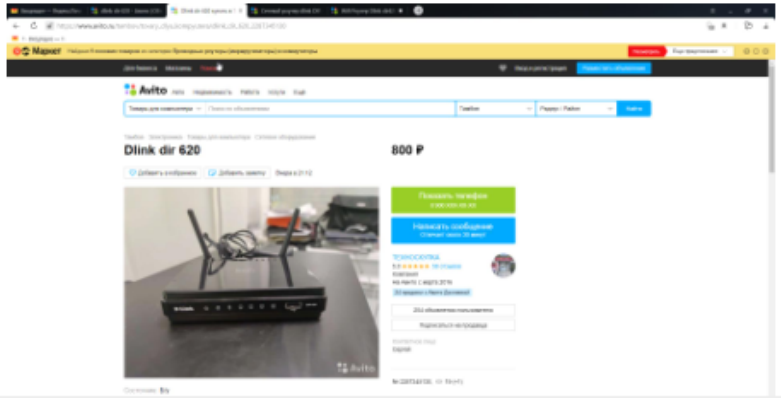
Поиск - Тип события

Операции с файлами 171

Всего: 1 , событий: 171

Время	Компьютер	Пользователь	Приложение	Операция	Устройство	Тип устройства	Имя файла	Тип устр. источни
					SCSI Disk Device		Word.docx	
2023-05-30 09:16:37 +4	DESKTOP-U0BRDOG	Валера	explorer.exe	Перемещение	VMware Virtual disk SCSI Disk Device	Hard	Другой документ с печатью.pdf	Hard
2023-04-21 17:35:51	DESKTOP-N36I35U	Ксения	explorer.exe	Удаление	VMware Virtual disk SCSI Disk Device	Hard	025.01.1220.0001.pdf	
2023-04-13 14:27:44	DESKTOP-N36I35U	Ксения	dllhost.exe	Удаление	VMware Virtual disk SCSI Disk Device	Hard	Тест договор — копия — копия.xlsx	
2023-04-13 14:27:40	DESKTOP-N36I35U	Ксения	explorer.exe	Удаление	VMware Virtual disk SCSI Disk Device	Hard	Тест договор — копия — копия.xlsx	
2023-04-13 14:19:45	DESKTOP-N36I35U	Ксения	explorer.exe	Перемещение	VMware Virtual disk SCSI Disk Device	Hard	Панель приборов правая.pdf	Hard
2023-04-13 14:19:45	DESKTOP-N36I35U	Ксения	explorer.exe	Перемещение	VMware Virtual disk SCSI Disk Device	Hard	5101070.pdf	Hard


Поиск - Сайт
youla.ru 44
drom.ru 33
avito.ru 29
vk.com 1
Всего: 4 , событий: 107
Сайт
Пользователь: Полное имя
Количество событий
44 youla.ru (41.1%)
33 drom.ru (30.8%)
29 avito.ru (27.1%)
1 vk.com (0.9%)
Андрей Тестов
Артём Слежкин
Андрей Тестов
Артём Слежкин
Андрей Тестов

Время	Тип	Компьютер	Пользователь	Приложение	Событие
					 Скачать Screenshot.jpg
2022-01-12 16:44:43	Время активности	DESKTOP-U0BRDOG	Валера	browser.exe	Dlink dir 620 купить в Тамбове | Бытовая электроника | Авито — Яндекс.Браузер Доски объявлений
2022-01-12 16:44:43	Снимок экрана	DESKTOP-U0BRDOG	Валера	browser.exe	Dlink dir 620 купить в Тамбове | Бытовая электроника | Авито — Яндекс.Браузер Screenshot.jpg 

Время 2022-01-12 16:44:52
Сервер Этот сервер
Заголовок окна dlink dir 620 - Авито | Объявления в России: недвижимость, транспорт, работа, услуги, вещи — Яндекс.Браузер
Приложение browser.exe
Тип события Время активности
Агент DESKTOP-U0BRDOG
Пользователь Валера
Посещение сайта https://www.avito.ru/rossiya?q=dlink+dir+620

staffcop

Актуальное законодательство

Уже есть

- Указ 250: персональная ответственность руководителя за состояние ИБ в организации
- ФЗ 152: необходимо сообщить об инциденте утечки ПДн в течение суток
- ФЗ 152: необходимо предоставить результаты расследования инцидента утечки ПДн в течение трёх суток
- ФЗ 187: ряд обязательных мер для предприятий КИИ

Готовятся

- Оборотные штрафы за утечку ПДн
- Уголовная ответственность за «продажу» ПДн
- Правительство само будет определять объекты КИИ

«За безопасность необходимо платить, а за ее отсутствие - расплачиваться»
/ Уинстон Черчилль /

Спасибо за внимание!

Николай Сухотерин

Специалист по внедрению

ООО «АТОМ БЕЗОПАСНОСТЬ»

n.suhoterin@staffcop.ru

staffcop.ru

Telegram