



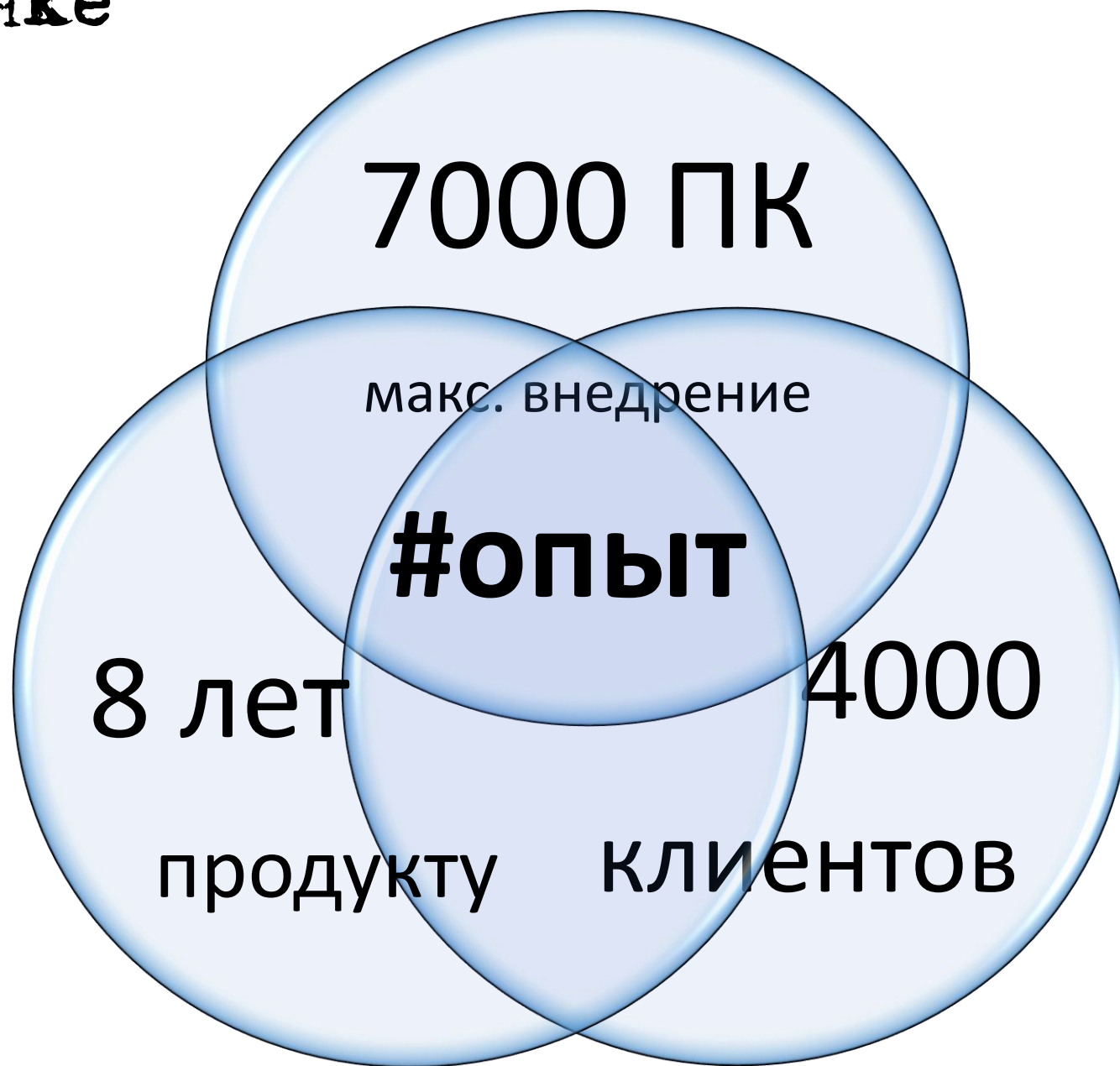
Технологии мониторинга и контроля

подозрительных действий сотрудников и
предотвращение утечки важной информации



#на рынке

Sk
ИТ



5.2

Инвентаризация ПО

Интеграция с AD

Голосовое DLP

Распознавание скриншотов

DLP компонент

Граф связей

Шаблоны угроз

Контроль отклонений

Отложенный мониторинг

64-битная редакция сервера

Нетипичное поведение

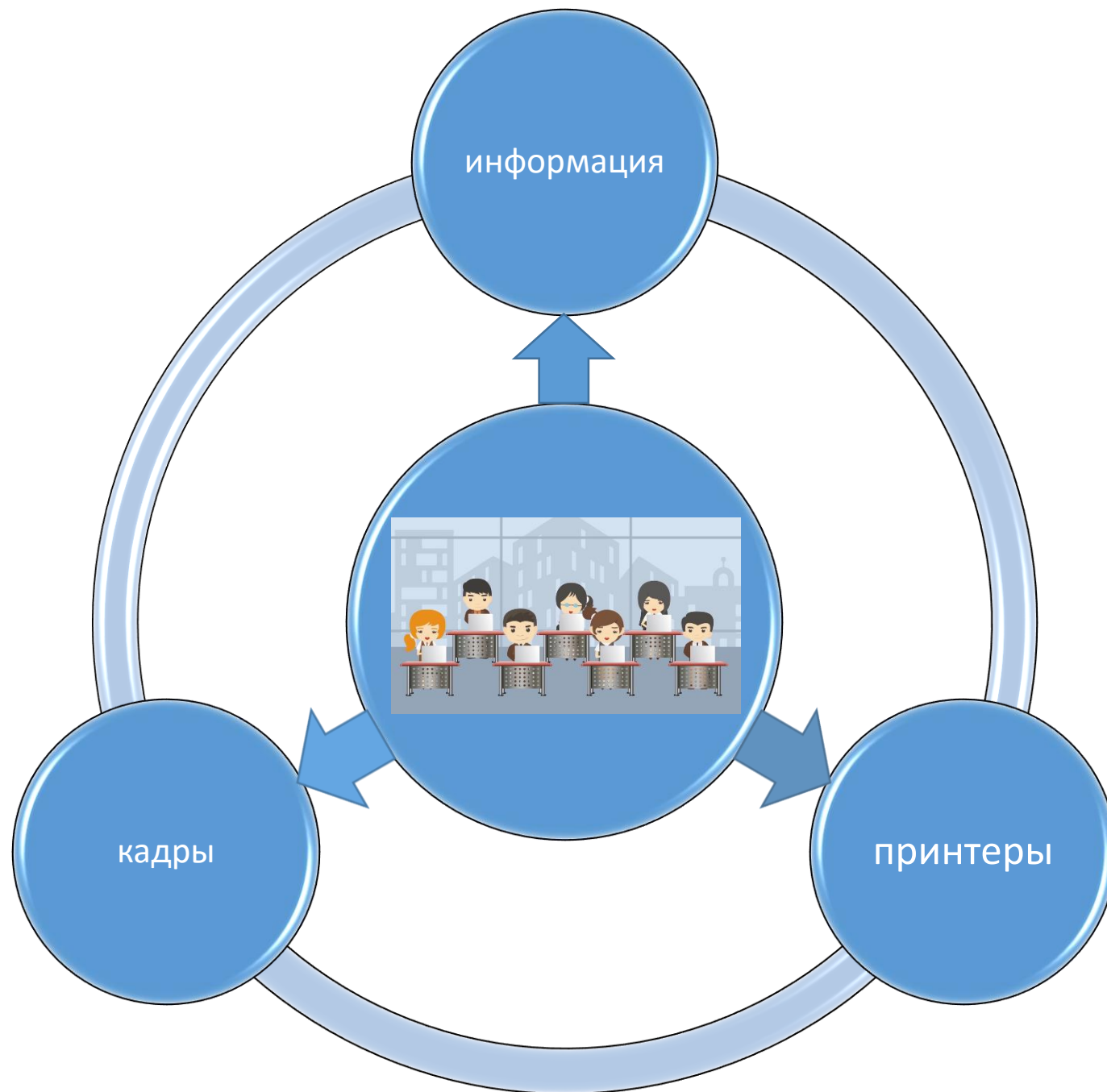
Проверка фальсификации данных численных отчетов

Скриншоты изменений в конкретных приложениях

6.1
установка «в один клик»



#риски



#контекст

- Выявление активностей в компании
- Представление

Стахановец

- Быстрое локальное расследование
- Принятие решений

Администрация

Администрация

- Контроль улучшений,
- Продуктивности и Вовлеченности

HR +
Консалтинг

- Обучение персонала
 - Разъяснение
 - Обучение Руководителей



#Отчеты

SHAPE

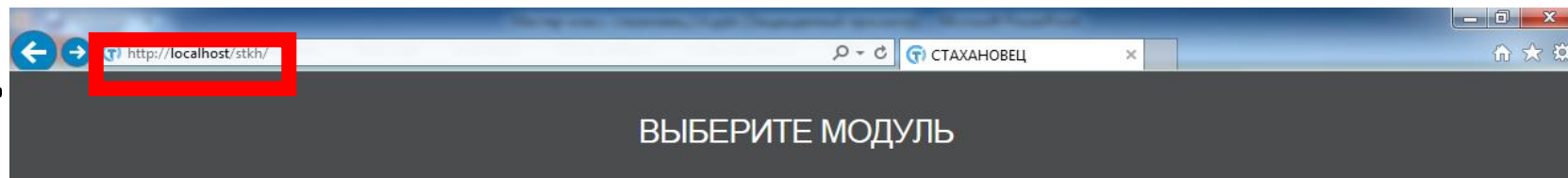
SPIN LOCK

 Стахановец



#ИНСТРУМЕНТЫ

1

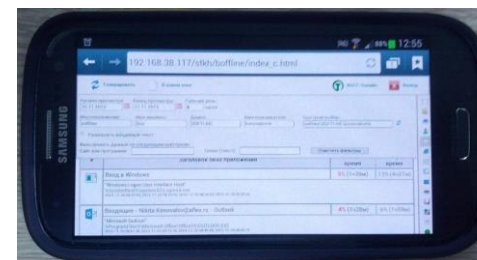


3



2

[Логотипы: вкл](#) | [Личный кабинет](#)



#расследование



1

Office\ERG-PIK\erg
Office\SCHERBAKOV\ceprey

3

Генерировать

4

2

МАСТЕР ОТЧЕТОВ

- Анализатор рисков
- Сводный отчет
- Машинное время
- Пользовательское время
- Программы
- Сайты
- Буфер обмена
- Интернет-запросы
- Снимки экранов
- Печать на принтере
- Файловые операции
- Отправка файлов
- Письма (e-mail)
- Чаты/звонки

От: 01.11.2014 00:00 До: 26.11.2014 24:00

Рабочий день: 9 Начало: 09:00 Перерыв: 60

☐ Развернуть свернутые блоки

Фильтр: сайт или программа

Фильтр: слово или текст

	по каждому	по группе
Анализатор рисков	☐	☒
Сводный отчет	☐	☒
Пользовательское время	☒	☒
Программы	☒	☒
Сайты	☒	☒
Буфер обмена	☒	☒
Интернет-запросы	☒	☒
Снимки экранов	☒	☐
Печать на принтере	☒	☒
Файловые операции	☒	☒
Отправка файлов	☒	☒
Письма (e-mail)	☒	☒
Чаты/звонки	☒	☒
Контакты	☐	☒
События: пользователь	☒	☒
GPS-трекинг	☒	☒

☒ Ускоренная генерация (ссылки на файлы теневого копирования)

☐ Ускоренная генерация (не показывать preview снимков экранов)

#обнаружение аномалий

1



2

3

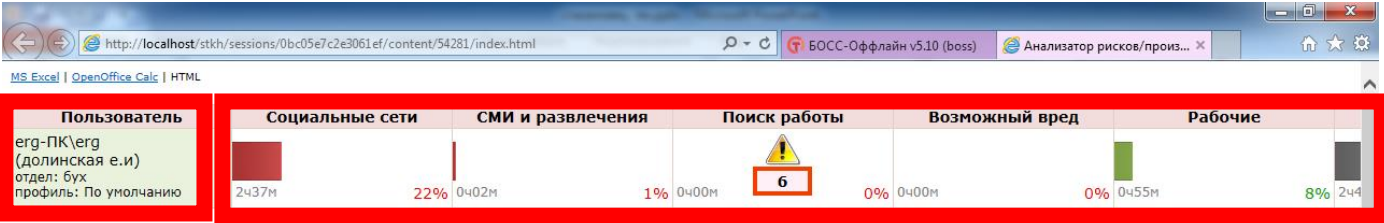


Категории Отклонения Ресурсы 4

msk.ru	7ч05м
Windows Logon User Interface Host	0ч56м
phoenixcontact.com	0ч07м
moscow.drom.ru	0ч06м
"Google Chrome"	0ч03м
"COM Surrogate"	0ч03м
"Калькулятор Windows"	0ч02м
metropoldevelopment.ru	0ч02м
arxbank.ru	0ч01м
yandex.ru	0ч01м
roel.ru	0ч01м

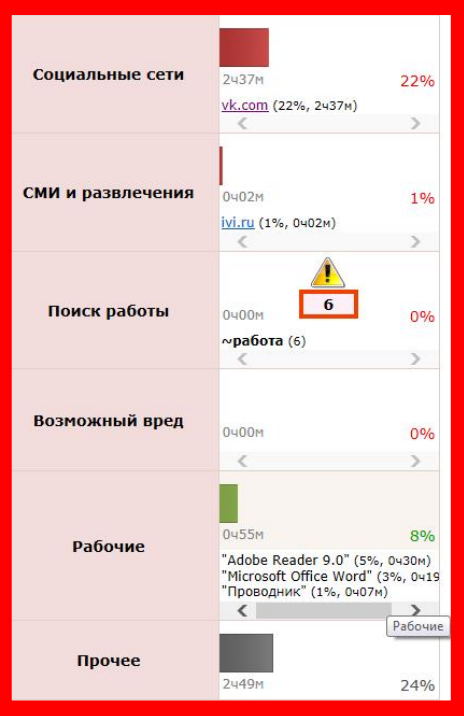
#обнаружение рисков

1

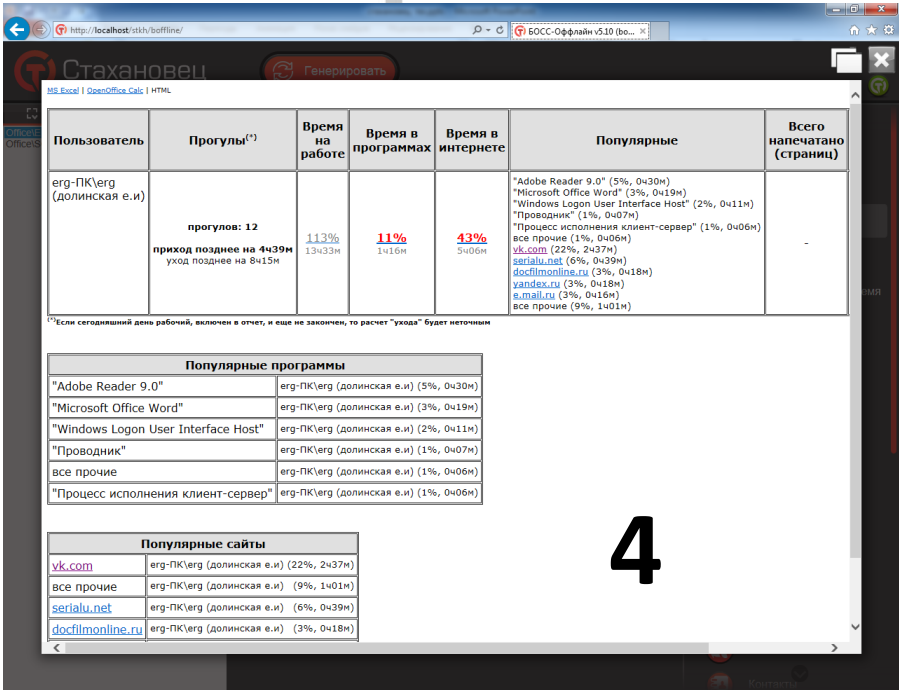


2

3

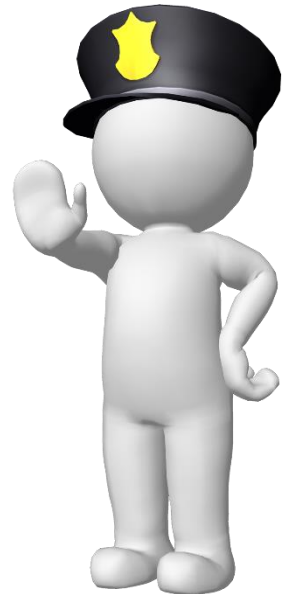
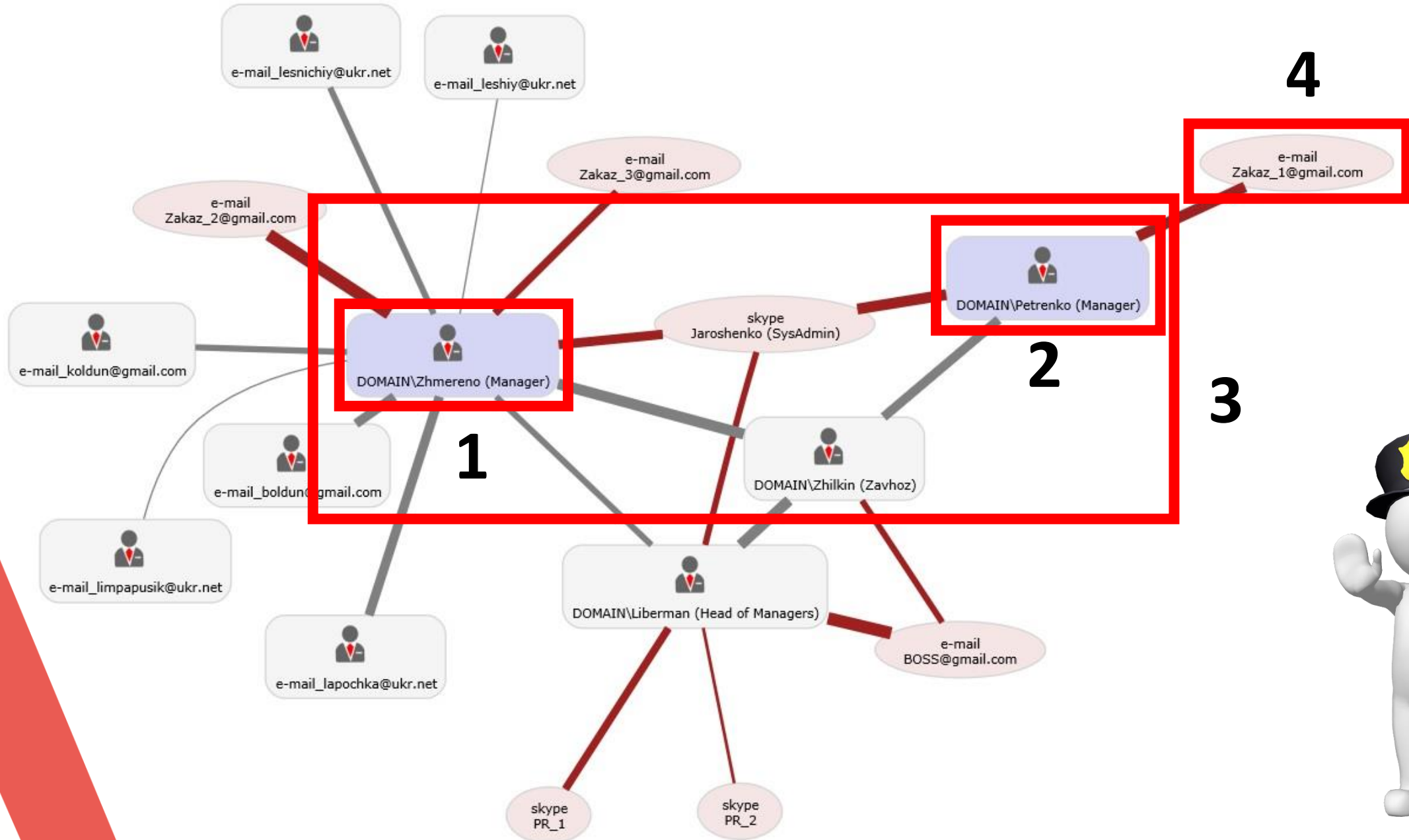


+ словарь наркомания



4

#обнаружение инсайдеров

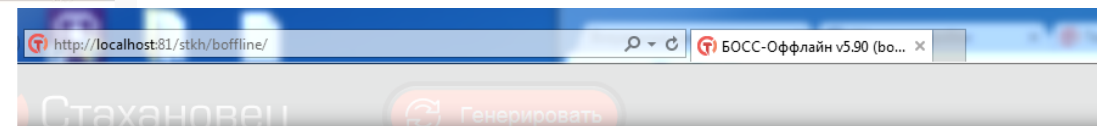
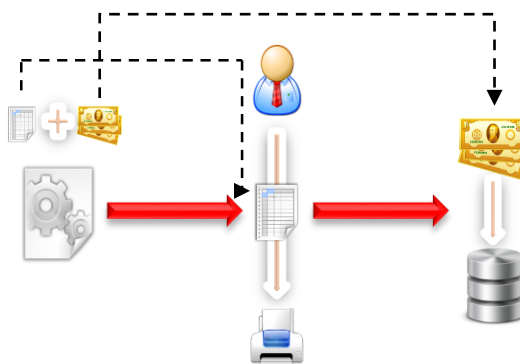


#другие риски

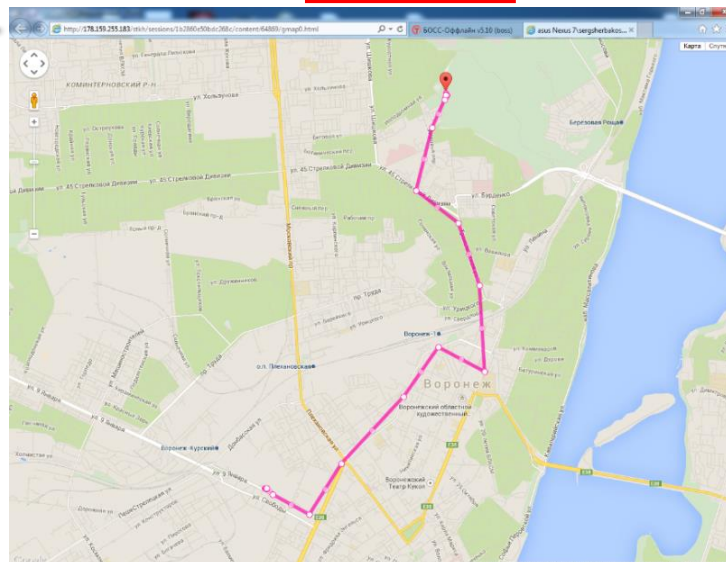
Подсказка: наведите указатель на восклицательный знак для просмотра сотрудников с похожим почерком в проблемном интервале

Подсказка: лучше строить данный отчет по группе сотрудников одного отдела с большим временным интервалом

Пользователь	День	Предупреждения
LAPTOP\Sergey (Годунов С.В.)	2015-02-01 (BC)	
1	2015-02-02 (ПН)	
	2015-02-03 (BT)	2
	2015-02-04 (CP)	

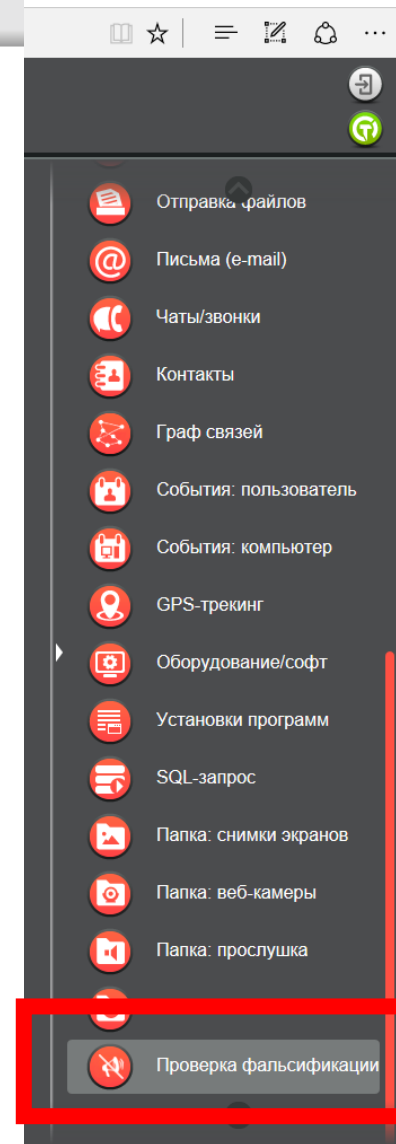
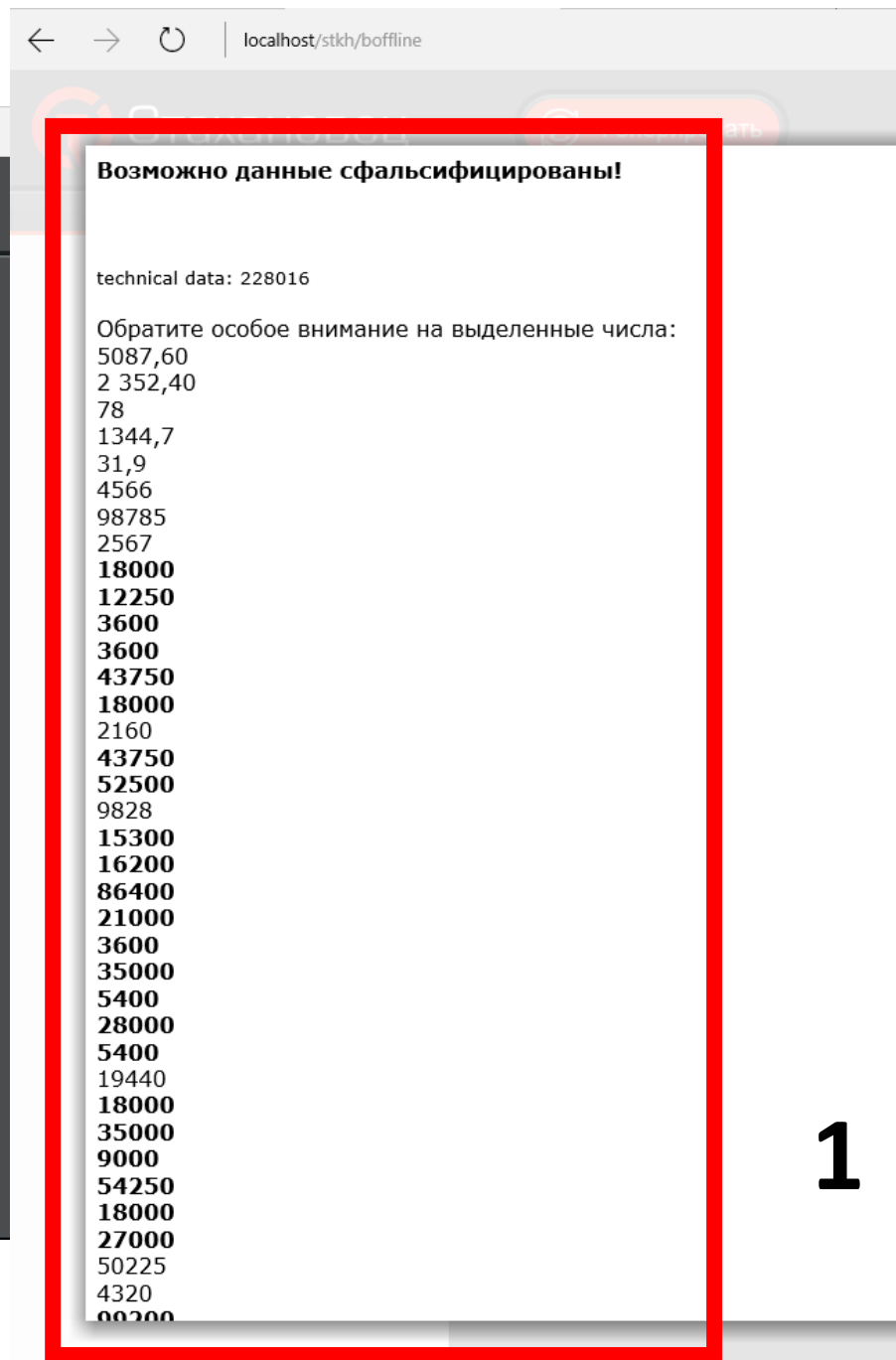
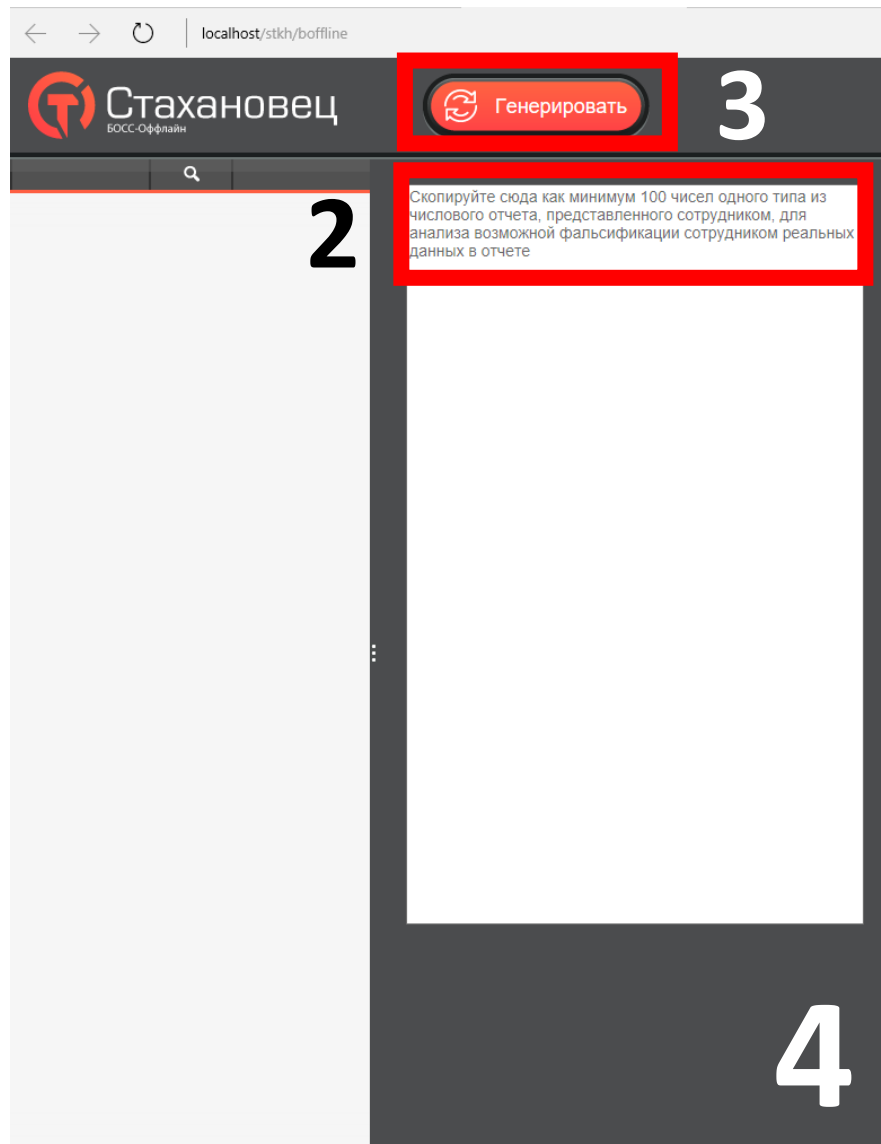


Пользователь	Время	Страниц	КБайт	Бумага	Цве	Документ	Принтер
Nikishin\Home (Иванов И.И.)	2016-02-16 12:23	1	22 КБ	A4 210x297		анкета_.xlsx 2016-02-16 12-23-59 00005.spl 2016-02-16 12-23-59 00005.shd 2016-02-16 12-23-59.jpg анкета_.xlsx	Canon LBP2900

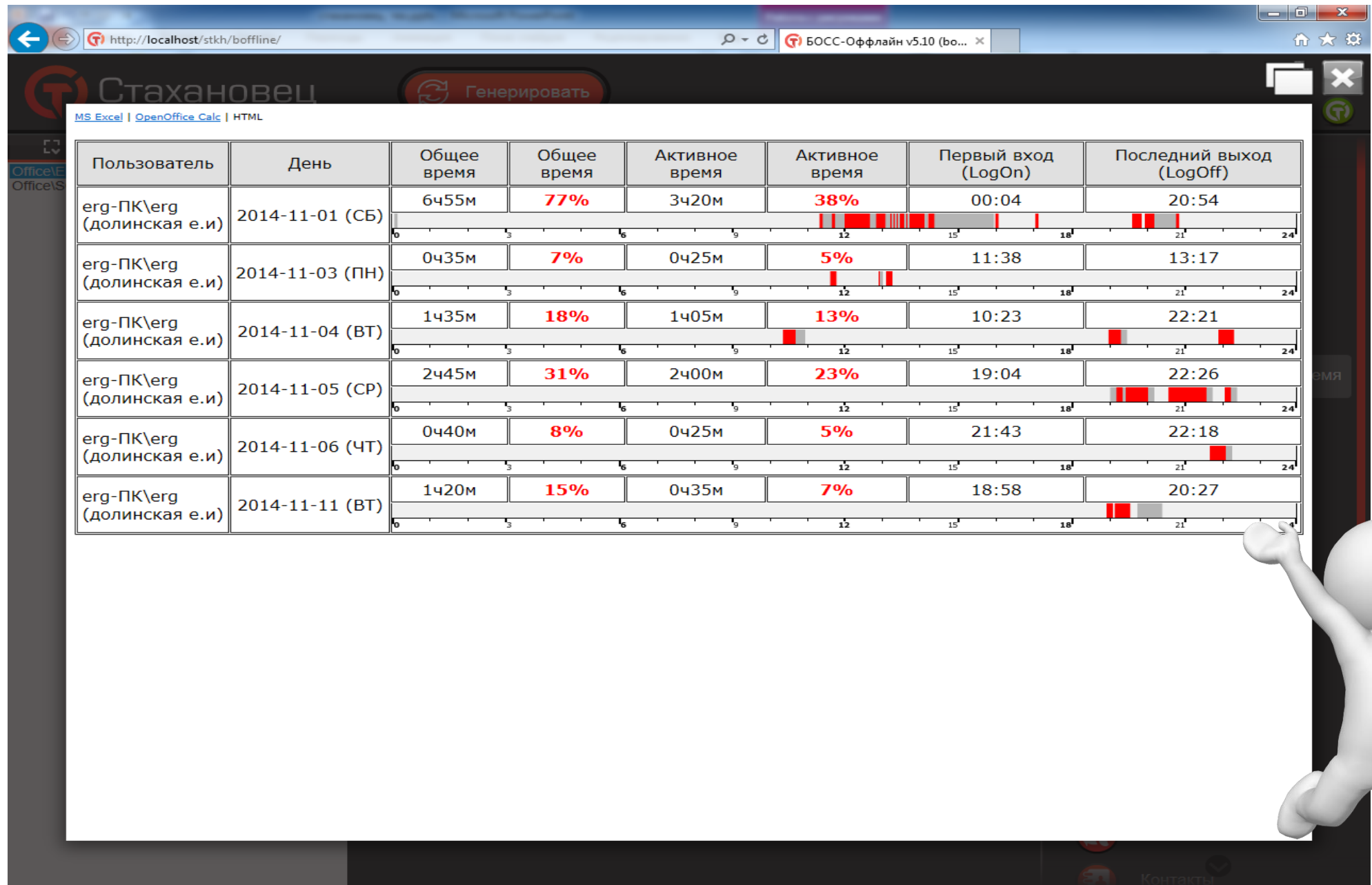


4

#финансовые риски



#ПОЛЬЗОВАТЕЛЬСКОЕ время



#программы

erg-ПК\erg (долинская е.и)

Суммарное время активной работы: ~ 3% (1435м)

#	Заголовок окна приложения	Активное время	Общее время
	16_metodika_raboty_v_sisteme_kpi_sf_supervayzer_upr_rab_otdela_v4.1.pdf - Ado... "Adobe Reader 9.0" %ProgramFiles%\Adobe\Reader 9.0\Reader\AcroRd32.exe 2014-11-05 19:55:15 Показать/скрыть вводимый текст	1% (0ч30м)	2% (0ч34м)
	Документ2 - Microsoft Word "Microsoft Office Word" %ProgramFiles%\Microsoft Office\OFFICE11\WINWORD.EXE 2014-11-05 20:47:21 Показать/скрыть вводимый текст	1% (0ч18м)	1% (0ч20м)
	Док фильм. В поисках правды. НЛО / The Truth Behind. UFOs (2011) - Google Chrome "Google Chrome" %ProgramFiles%\Google\Chrome\Application\chrome.exe 2014-11-01 11:23:33 Показать/скрыть вводимый текст	1% (0ч18м)	2% (0ч49м)
	Вход в Windows "Windows Logon User Interface Host" %SystemRoot%\system32\LogonUI.exe 2014-11-01 12:15:47, 2014-11-03 11:38:52, 2014-11-04 15:58:34, 2014-11-05 19:04:20, 2014-11-06 21:43:01, 2014-11-11 18:58:06	1% (0ч11м)	1% (0ч16м)
	Информация "Процесс исполнения клиент-сервер" %SystemRoot%\system32\csrss.exe 2014-11-11 19:51:24	1% (0ч05м)	1% (0ч29м)
	Новая вкладка - Google Chrome "Google Chrome" %ProgramFiles%\Google\Chrome\Application\chrome.exe 2014-11-01 12:16:15, 2014-11-03 11:39:34, 2014-11-03 12:57:24, 2014-11-03 12:57:27, 2014-11-04 10:27:50 Показать/скрыть вводимый текст	1% (0ч04м)	1% (0ч04м)
	485 - Фотоальбом Windows	1% (0ч04м)	1% (0ч04м)



#сайты

erg-ПК\erg (долинская е.и)

Суммарное время активной работы: ~ 9% (4ч50м)

#	Заголовок окна приложения	Активное время	Общее время
	Друзья Елены Долинской 169 друзей - Google Chrome	4% (2ч08м)	7% (3ч20м)

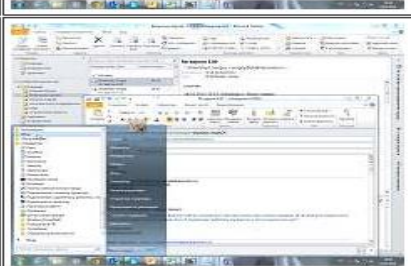
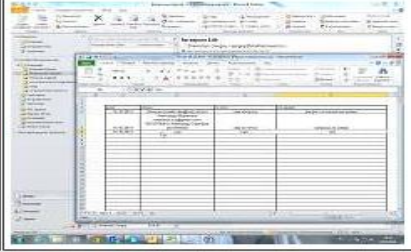
2014-11-01 12:18:35, 2014-11-03 11:39:45, 2014-11-03 12:50:52, 2014-11-04 10:31:24, 2014-11-05 19:52:03, 2014-11-11 19:01:54
<https://vk.com/friends>
2014-11-01 12:18:46, 2014-11-06 21:49:54
<https://vk.com/video>
2014-11-01 12:18:53, 2014-11-01 12:18:55
<https://vk.com/video?q=%D0%BA%D0%BB%D0%B8%D1%87%D0%BA%D0%BE§ion=search>
2014-11-01 13:58:19, 2014-11-03 12:51:08, 2014-11-04 10:31:33, 2014-11-05 19:39:21
<https://vk.com/feed>
2014-11-01 14:00:39, 2014-11-03 12:55:49, 2014-11-04 22:20:29
<https://vk.com/groups>
2014-11-01 14:15:23, 2014-11-03 11:40:01, 2014-11-03 13:12:39, 2014-11-04 21:57:09
<https://vk.com/im>
2014-11-01 14:15:59, 2014-11-03 12:51:17, 2014-11-04 10:31:36
<https://vk.com/feed?section=photos>
2014-11-01 14:18:32
<https://vk.com/alonedevil>
2014-11-01 14:18:46
<https://vk.com/banzaika>
2014-11-01 14:19:25
<https://vk.com/ruda915>
2014-11-01 14:20:28
<https://vk.com/audios146221651>
2014-11-03 12:55:52, 2014-11-04 22:20:32
<https://vk.com/mollisshop>
2014-11-03 12:56:32
<https://vk.com/i.kino>
2014-11-04 10:32:48
<https://vk.com/id83336927>
2014-11-04 10:33:16, 2014-11-05 19:19:11, 2014-11-05 19:19:16, 2014-11-05 19:49:15
<https://vk.com/id146221651>
2014-11-04 19:15:33, 2014-11-04 19:15:40
<https://vk.com/friends?section=online>
2014-11-04 21:58:47
<https://vk.com/friends?id=146221651§ion=online>
2014-11-04 21:59:25
<https://vk.com/im?sel=7672455>
2014-11-05 19:40:53
<https://vk.com/feed?section=updates>
2014-11-05 21:22:00
<https://vk.com/superskayasvadba>
2014-11-05 21:23:45, 2014-11-05 21:23:55
https://vk.com/makeme_beauty
2014-11-05 21:26:43
<https://vk.com/escanlee>
2014-11-06 21:48:22
<https://vk.com/id271184829>
2014-11-06 21:49:55



#скриншоты

http://localhost/stkh/boffline/ БОСС-Оффлайн v5.10 (bo... x

Стахановец Генерировать

Scherbakov\сергей (щербаков)	2014-10-16 10:20:44 (ЧТ)	
Scherbakov\сергей (щербаков)	2014-10-16 10:21:45 (ЧТ)	
Scherbakov\сергей (щербаков)	2014-10-16 10:22:45 (ЧТ)	
Scherbakov\сергей (щербаков)	2014-10-16 10:23:46 (ЧТ)	

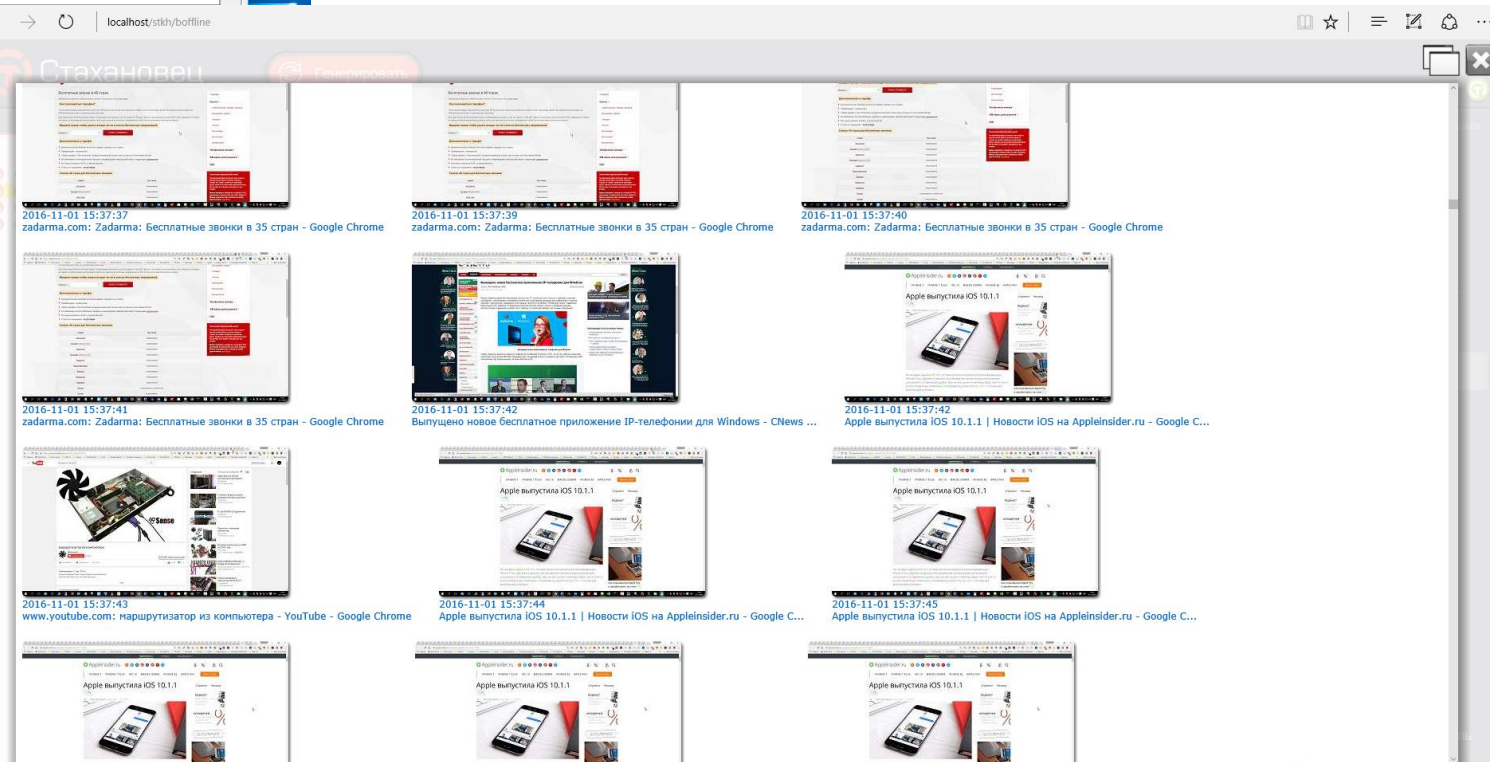
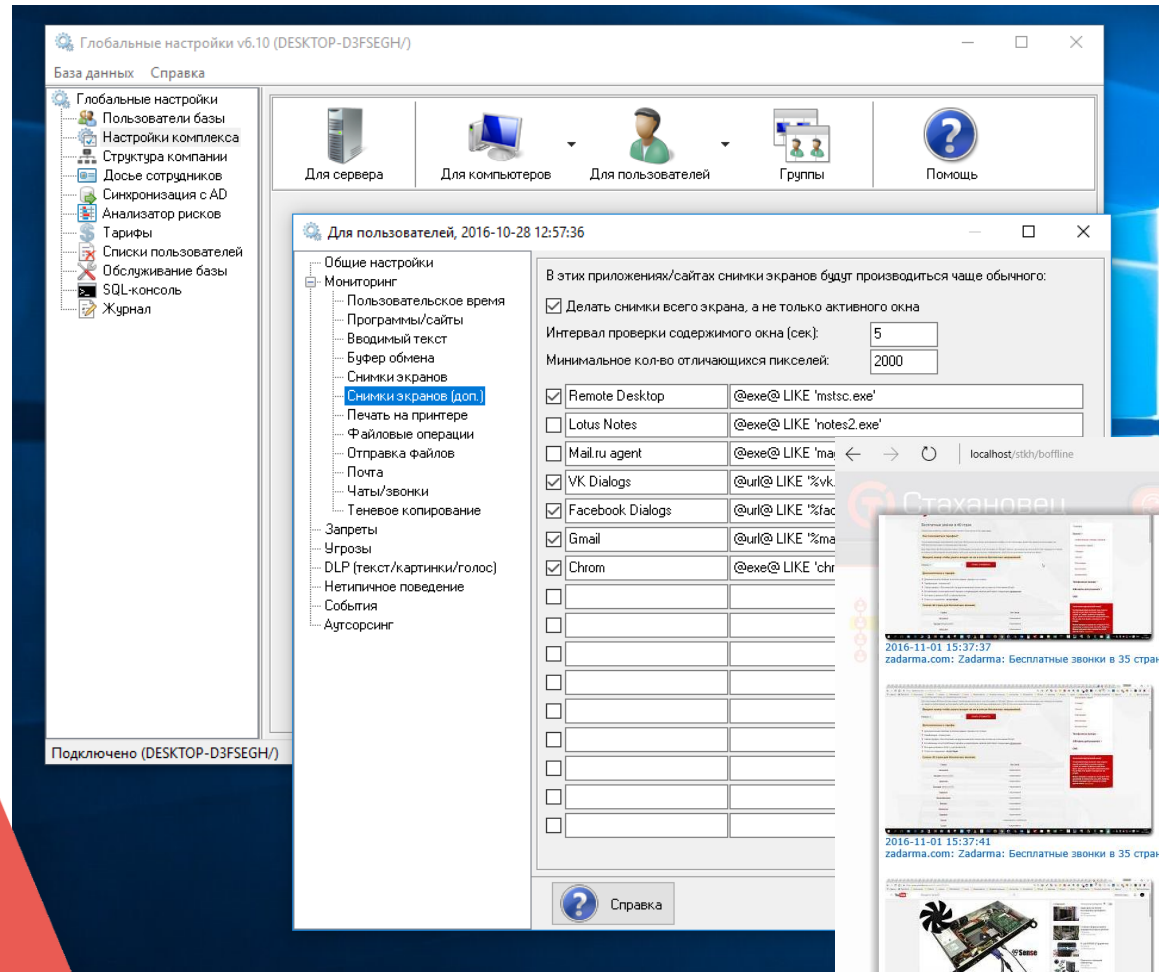
Office\B Office\B

мя

Контакты



#СКРИНШОТЫ ДОП. (ИЗМЕНЕНИЯ В ПРИЛОЖЕНИИ)



ВИДЕО ИЗ СКРИНШОТОВ

 **Стахановец**
БОСС-Офлайн

Генерировать

От: 01.11.2016 10:00 До: 01.11.2016 18:00

DESKTOP-NQVDO2NMisha-PB @ DESKTOP-NC
HostMisha-Host @ HOST.WORKGROUP
MOBILEnost79_gmail.com @ XIAOMI-MI-4C.MOE
Новый отдел2Иванов И.И. @ MISHA-PB.WORK

localhost/stkhy/boffline

2016-11-01 15:53:11, www.youtube.com: маршрутизатор из компьютера - YouTube - Google Chrome



маршрутизатор из компьютера

Нитрохелус

54 608 просмотров

Опубликовано: 17 авг. 2015 г.

Скачать pfsense <https://www.pfsense.org/download/>
Группа в ВК https://vk.com/free_pfsense

Следующее

Автопроизводство

Один день из жизни монтажника проводного

Стильная сборка сетевого маршрутизатора на pfSense

D Link DIR300 b7 доработка

Принесли сгоревший компьютер

Игровой компьютер на AMD из 2003 года

КВАНТОВЫЙ ПЕРЕХОД. I ч.

Чиним брендовый компьютер DEPO Part 1

1:05:59

1:33:58

Пользовательское время

Программы

Сайты

Буфер обмена

Клавиатурный почерк

Интернет-запросы

Снимки экранов

Видео снимков

Печать на принтере

Файловые операции

Отправка файлов

Письма (e-mail)

Чаты/звонки

Контакты

Граф связей

События: пользователь

События: компьютер

#Отправка файлов

← → http://localhost/stkh/boffline/ БОСС-Оффлайн v5.10 (bo... ×

Стахановец Генерировать

Пользователь	Время	Файл/Информация
Scherbakov\сергей (щербачков)	2014-11-11 15:08	C:\Users\сергей\Desktop\файловые операции отчет.png Drag (lync.exe)
Всего файлов: 3	2014-11-25 15:14	C:\Users\сергей\Desktop\Шаблоны заявлений на ежегодный оплачиваемый отпуск (1).xlsx (lync.exe)

Шаблоны заявлений на ежегодный оплачиваемый отпуск (1).xlsx - Microsoft Excel

Файл Главная Вставка Разметка страницы Формулы Данные Рецензирование Вид

Вставить Шрифт Выравнивание Число

ЗАЯВЛЕНИЕ																
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
ЗАЯВЛЕНИЕ																
Прошу предоставить мне ежегодный оплачиваемый отпуск в период																
с " " 20 г. по " " 20 г.																
/ " " 20 г.																
Страница 1																
СОГЛАСОВАНО																
Руководитель																
/ " " 2																



#ПИСЬМА

2014-11-11 16:13	sergey@stakhanovets.ru	Re: Версия продукта 1.99
2014-11-11 16:14	Sergey Pavlovich ukrkiev@ukr.net	2014-11-11 16-14-04 0.msg (408 KB) RE: Re [2]: Re [2]: Re [2]: Re [2]
2014-11-11 16:14	ukrkiev@ukr.net no.reply@ukr.net	2014-11-11 16-14-19 0.msg (52 KB) Autoreply from ukrkiev@ukr.net
2014-11-11 16:16	Sapronov, Stanislav /O=SOFTLINE/OU=EXCHANGE ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=SAPRONOV STANISLAVD3C	2014-11-11 16-16-14 0.msg без темы
2014-11-11 16:19	Stakhanovets Support support@probusinesslab.com	2014-11-11 16-19-18 0.msg Сгенерирован клиент
2014-11-13 12:14	PFB Matskiv Andriy Andriy.Matskiv@profinbank.com	2014-11-13 12-14-14 0.msg IE
2014-11-13 12:35	PFB Matskiv Andriy Andriy.Matskiv@profinbank.com	2014-11-13 12-35-35 0.msg RE: IE
2014-11-13 12:51	Шмаков Павел Викторович ShmakovPV@pgkweb.ru	2014-11-13 12-51-51 0.msg звук
2014-11-13 12:52	Бавария x962@serverfreewww3.com	2014-11-13 12-52-35 0.msg [SPAM] Немецкий самодельный аппарат
2014-11-13 12:54	Шмаков Павел Викторович ShmakovPV@pgkweb.ru	2014-11-13 12-54-40 0.msg RE: звук
2014-11-13 12:55	Corporate University /O=SOFTLINE/OU=MOSCOW/CN=RECIPIENTS/CN=LABTEST	2014-11-13 12-55-47 0.msg (1 KB) Подарки для детей сотрудников к Новому году
2014-11-13 13:05	Smirnova, Anastasiya /O=SOFTLINE/OU=EXCHANGE ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=SMIRNOVA ANASTASIYA	2014-11-13 13-05-33 0.msg (68 KB) Подарки для детей сотрудников к Новому году
2014-11-13 13:46	Ryzhkov, Aleksey /O=SOFTLINE/OU=EXCHANGE ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=ALEKSEYRZH	2014-11-13 13-46-16 0.msg (156 KB) Re: Подарки для детей сотрудников к Новому году
2014-11-13 14:04	spoler spoler bbk2000@mail.ru	2014-11-13 14-04-05 0.msg (52 KB) Ок
2014-11-13 14:09	PFB Matskiv Andriy Andriy.Matskiv@profinbank.com	2014-11-13 14-09-11 0.msg (104 KB) RE: IE
2014-11-13 14:12	Shamshyn, Sergey sergey@stakhanovets.ru	2014-11-13 14-12-32 0.msg (64 KB) Браузер
2014-11-13 14:17	spoler spoler bbk2000@mail.ru	2014-11-13 14-17-49 0.msg (72 KB) RE: Ок
2014-11-13 14:18	sibstrin-mgr sibstrin-mgr@yandex.ru	2014-11-13 14-18-03 0.msg (52 KB) По установке программы Стахановец
2014-11-13 14:21	spoler spoler bbk2000@mail.ru	2014-11-13 14-21-32 0.msg (48 KB) RE: Ок
2014-11-13 14:23	sibstrin-mgr sibstrin-mgr@yandex.ru	2014-11-13 14-23-31 0.msg (48 KB) RE: По установке программы Стахановец
2014-11-13 14:28	bbk2000@mail.ru	2014-11-13 14-28-16 0.msg (56 KB) FW: Ок
2014-11-13 14:28	Murashova, Anna /o=SOFTLINE/ou=Exchange Administrative Group/cn=Recipients/cn=Murashova Anna	2014-11-13 14-28-55 0.msg (92 KB) RE: клиент по стахановцу
2014-11-25 14:45	Scherbakov, Sergey /o=SOFTLINE/ou=Exchange Administrative Group/cn=Recipients/cn=1ba2d11bedc24cf38cc9c177356d0caf-Scherbakov Serg	2014-11-25 14-45-06 0.msg (80 KB) RE: стахановец 4.99
2014-11-25 14:45	Scherbakov, Sergey /O=SOFTLINE/OU=EXCHANGE ADMINISTRATIVE GROUP/CN=RECIPIENTS/CN=1BA2D11BEDC24CF38CC9C177356D0CAF-SCHERBAKOV SERG	2014-11-25 14-45-07 0.msg (96 KB) RE: стахановец 4.99
2014-11-25 14:45	vega_adm@3ar.su	2014-11-25 14-45-23 0.msg (76 KB) RE: стахановец 4.99
2014-11-25 14:55	(Textile & Group Industry) silver.tex@aol.com	2014-11-25 14-55-21 0.msg (64 KB) [SPAM] Mr. Silver



#ЧАТЫ ##ЗВОНКИ

http://localhost/stkh/boffline/ БОСС-Оффлайн v5.10 (bo... x

Генерировать

Office\B
Office\B

Щербаков 2014-11-11 14:29:10
ВЫЗОВ ЗАВЕРШЕН tel:+79178282552 (0:00:09)
[2014-11-11 14 29 01.ogg](#)

Щербаков 2014-11-11 14:29:25
ИСХОДЯЩИЙ ВЫЗОВ tel:+79178282552

Щербаков 2014-11-11 14:30:05
ВЫЗОВ ЗАВЕРШЕН tel:+79178282552 (0:00:39)
[2014-11-11 14 29 25.ogg](#)

Щербаков 2014-11-11 13:54:47
ВЫЗОВ ЗАВЕРШЕН tel:+79237717337 (0:30:15)
[2014-11-11 13 24 32.ogg](#)
[2014-11-11 13 24 32 1.ogg](#)
[2014-11-11 13 24 32 2.ogg](#)
[2014-11-11 13 24 32 3.ogg](#)

Щербаков 2014-10-08 15:01:14
ИСХОДЯЩИЙ ВЫЗОВ tel:+79857740088

Щербаков 2014-10-08 15:14:14

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:24:49
отправила ему ключи

Щербаков 2014-10-10 09:24:50
линк тупит)))

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:24:53
он написал мне

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:24:59
ааа)))

Щербаков 2014-10-10 09:25:10
уже с ключами он да))))

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:25:26
дозвониться не могла, отправила и по почте написала

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:25:41
он не говорил сколько у них всего?

sip:alena.minakova@aflex.ru (Lync) 2014-10-10 09:25:50
?

Щербаков 2014-10-10 09:26:08
30-50

Щербаков 2014-10-10 09:26:12
)))

Контакты



#КОНТАКТЫ

http://localhost/stkh/boffline/ БОСС-Офлайн v5.10 (bo... x

Стахановец Генерировать

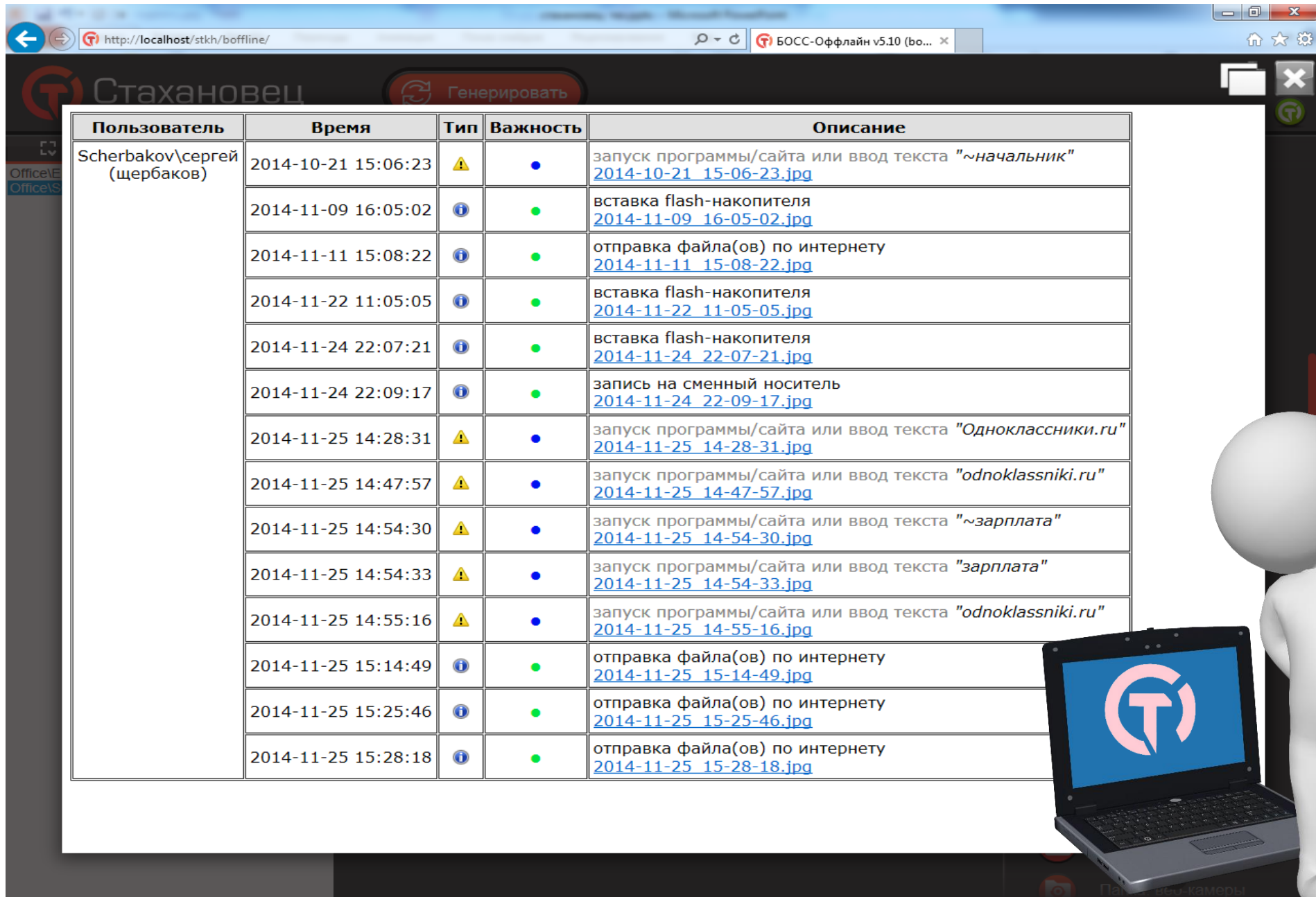
OfficeE OfficeS

Заккрыть

Пользователь	Контакт	Сотрудник	Кол-во	Тип
Scherbakov\сергей (щербачков) Всего контактов: 51	19:ac35032ff7384f37a75666211890c2be@thread.skype		336	Skype
	sip:roman.voroshilin@aflex.ru	долинская е.и	137	Lync
	sip:alena.minakova@aflex.ru		65	Lync
	nedobrityi_burunduk		50	Skype
	tipi-top32		37	Skype
	19:0ab2fc44cd0549249a002c83fbd72ddd@thread.skype		35	Skype
	sergey@stakhanovets.ru		21	e-mail
	ukrkiev@ukr.net		20	e-mail
	protatai		16	Skype
	no.reply@ukr.net		10	e-mail
	tatyanochka_m		10	Skype
	tel: +79178282552		8	Lync
	#serg9876543211/\$*T;8412		7	Skype
	sip:k.kor@softlinegroup.com		7	Lync
	bastitgru		7	Skype
	romanticlove_		7	Lync
	sip:e.tsu@softlinegroup.com		7	Lync
	19:679bf33ec68d48ae93d518f476ec849c@thread.skype		6	Skype
	lion_k77		5	Skype
	sip:stanislav.sapronov@aflex.ru		4	Lync
	bbk2000@mail.ru		4	e-mail
	ShmakovPV@pgkweb.ru		3	e-mail
	990099@bk.ru		3	e-mail
	Andriy.Matskiv@profinbank.com		3	e-mail
	tel: +74995034004		2	Lync

Панка вы-камеры

#СОБЫТИЯ: ПОЛЬЗОВАТЕЛЬ



Пользователь	Время	Тип	Важность	Описание
Scherbakov\сергей (щербаков)	2014-10-21 15:06:23	⚠	●	запуск программы/сайта или ввод текста "начальник" 2014-10-21 15-06-23.jpg
	2014-11-09 16:05:02	ℹ	●	вставка flash-накопителя 2014-11-09 16-05-02.jpg
	2014-11-11 15:08:22	ℹ	●	отправка файла(ов) по интернету 2014-11-11 15-08-22.jpg
	2014-11-22 11:05:05	ℹ	●	вставка flash-накопителя 2014-11-22 11-05-05.jpg
	2014-11-24 22:07:21	ℹ	●	вставка flash-накопителя 2014-11-24 22-07-21.jpg
	2014-11-24 22:09:17	ℹ	●	запись на сменный носитель 2014-11-24 22-09-17.jpg
	2014-11-25 14:28:31	⚠	●	запуск программы/сайта или ввод текста "Одноклассники.ru" 2014-11-25 14-28-31.jpg
	2014-11-25 14:47:57	⚠	●	запуск программы/сайта или ввод текста "odnoklassniki.ru" 2014-11-25 14-47-57.jpg
	2014-11-25 14:54:30	⚠	●	запуск программы/сайта или ввод текста "зарплата" 2014-11-25 14-54-30.jpg
	2014-11-25 14:54:33	⚠	●	запуск программы/сайта или ввод текста "зарплата" 2014-11-25 14-54-33.jpg
	2014-11-25 14:55:16	⚠	●	запуск программы/сайта или ввод текста "odnoklassniki.ru" 2014-11-25 14-55-16.jpg
	2014-11-25 15:14:49	ℹ	●	отправка файла(ов) по интернету 2014-11-25 15-14-49.jpg
	2014-11-25 15:25:46	ℹ	●	отправка файла(ов) по интернету 2014-11-25 15-25-46.jpg
	2014-11-25 15:28:18	ℹ	●	отправка файла(ов) по интернету 2014-11-25 15-28-18.jpg



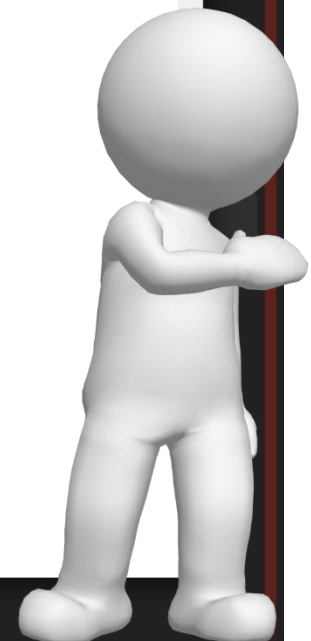
[illegible]

#оборудование и ПО

http://localhost/stkh/boffline/ БОСС-Оффлайн v5.10 (bo... x

Генерировать

	<pre>RegisteredUser = "erg" SerialNumber = "89572-OEM-7332166-00026" Version = "6.0.6001" }; [2014-10-29] (удалено) Процессор { Description = "x64 Family 6 Model 23 Stepping 10" Caption = "x64 Family 6 Model 23 Stepping 10" Name = "Pentium(R) Dual-Core CPU T4200 @ 2.00GHz" Manufacturer = "GenuineIntel" DeviceID = "CPU0" MaxClockSpeed = "2000" NumberOfCores = "2" NumberOfLogicalProcessors = "2" ProcessorId = "BFEBFBFF0001067A" SocketDesignation = "Socket 478" Version = "Model 7, Stepping 10" }; [2014-10-30] (добавлено) Процессор { Description = "x64 Family 6 Model 23 Stepping 10" Caption = "x64 Family 6 Model 23 Stepping 10" Name = "Pentium(R) Dual-Core CPU T4200 @ 2.00GHz" Manufacturer = "GenuineIntel" DeviceID = "CPU0" MaxClockSpeed = "2000" NumberOfCores = "2" NumberOfLogicalProcessors = "2" ProcessorId = "BFEBFBFF0001067A" SocketDesignation = "Socket 478" Version = "Model 7, Stepping 10" };</pre>
Office\SCHERBAKOV	<pre>[2014-10-08] Процессор { Description = "AMD64 Family 16 Model 5 Stepping 2" Caption = "AMD64 Family 16 Model 5 Stepping 2" Name = "AMD Athlon(tm) II X4 620 Processor" Manufacturer = "AuthenticAMD" DeviceID = "CPU0" MaxClockSpeed = "2600" NumberOfCores = "4" NumberOfLogicalProcessors = "4" ProcessorId = "178BFBFF00100F52" SocketDesignation = "CPUSocket" Version = "Model 5, Stepping 2" }; [2014-10-08] Материнская плата { Description = "Base Board" Caption = "Base Board"</pre>



#МОНИТОРИНГ

3

1

Стахановец
БОСС-Онлайн

Общие сведения | **Список процессов/окон** | Экраны пользователей | Изображения с веб-камер | Наблюдение экранов | Наблюдение с веб-камер | Прослушка | Текстовая речь | Пауза/наблюдение

Офис
Computers
Сотрудники

Дарья - Входящие - Outlook
Евгений
Константин - Диалоги - Google Chrome
Нина - Outlook
Роман - RE: Skype for business - Сообщение (HTML)
Светлана
Отдел продаж/Пётр - Входящие -
JAMIL_LOGOFF_@JAMIL
JONNY_LOGOFF_@JONNY

201 -03-21 16:52:38
\m.stryjakov @ DC1.
запуск программы/сайта или ввод текста "@EMAIL: @mail.ru"
201 -03-21 16:51:42
(Светлана):
запуск программы/сайта или ввод текста "@EMAIL: -----admin@sharly-fashion.ru"
201 -03-21 16:50:40
\m.stryjakov @ DC1.
запуск программы/сайта или ввод текста "@EMAIL: @mail.ruLjDlj"
201 -03-21 16:49:04
\m.stryjakov @ DC1.
запуск программы/сайта или ввод текста "@PHONE: 495)785-"
Список текущих событий

2



5

Внимание!
2014-11-25 14:55:16
Office\Scherbakov\сергей (щербakov):
запуск программы/сайта или ввод текста "odnoklassniki.ru"
2014-11-25 14:54:33
Office\Scherbakov\сергей (щербakov):
запуск программы/сайта или ввод текста "зарплата"
2014-11-25 14:54:30
Office\Scherbakov\сергей (щербakov):
запуск программы/сайта или ввод текста "~зарплата"

4

Внимание!
2014-11-25 14:55:16
Office\Scherbakov\сергей (щербakov):
запуск программы/сайта или ввод текста "odnoklassniki.ru"

RU 14:55 25.11.2014

#мониторинг #Видео #stream

2

Стахановец
БОСС-Онлайн

Общие сведения
Список процессов/окон
Экраны пользователей
Изображения с веб-камер
Наблюдение экранов
Наблюдение с веб-камер
Прослушка
Пауза/возоб. наблюдения
Послать сообщение
Обновить клиентское ПО
Удалить клиентское ПО

1

laptop-02\laptop LAPTOP-02.WORKGROUP - (правый клик - меню)

3

ЛAPTOP-02.WORKGROUP - (правый клик - меню)

1 онлайн-пользователей

#МОНИТОРИНГ #audio #stream

1

The screenshot shows the 'Стахановец' BOSS-Online v5.10 (boss) interface. The top navigation bar includes icons for 'Общие сведения', 'Список процессов/окон', 'Экраны пользователей', 'Изображения с веб-камер', 'Наблюдение экранов', 'Наблюдение с веб-камер', 'Прослушка' (highlighted with a red box and labeled '2'), and 'Пауза/возобновление наблюдения'. Below the navigation bar, a list of online users is displayed, with 'SCHERBAKOV (192.168.1.3)' highlighted in a yellow box and a red border (labeled '1'). To the right, a log of activities is shown, including timestamps and user actions like 'запуск программы/сайта или ввод текста "odnoklassniki.ru"'. A 3D white figure holding a red megaphone is positioned over the user list. At the bottom, a status bar indicates '1 онлайн-компьютеров / 1 онлайн-пользователей'.

3

The screenshot shows a window titled 'Office\SCHERBAKOV - Прослушивание'. It displays two audio level meters. The top meter is labeled 'Громкость: 0 dB (используйте SHIFT +/- для изменения)' and the bottom meter is labeled 'Громкость: 0 dB (используйте CTRL +/- для изменения)'. Both meters show a green bar indicating the current audio level. At the bottom right, there is a button labeled 'F12 - запись в файл'.

#структура



#Нагрузка

КОЛИЧЕСТВО ПК = 50

Рост БД

- Хранение данных **60 дней.**
- Объем базы данных (Прим.) **900 Мб**
- Видео и аудио данные не записываются в БД
- Периодически создание скриншотов

ПРИ ТАКИХ ПОКАЗАТЕЛЯХ РОСТ БАЗЫ ДАННЫХ НЕ НАБЛЮДАЕТСЯ

НАГРУЗКА НА СЕТЬ

Общий мониторинг + скриншоты + видео

Path	Size	PhysicalAd
C:\windows\system32\sqmapi.dll	76 K	
C:\windows\system32\srchadmin.dll	176 K	
C:\windows\system32\srvccli.dll	116 K	
C:\windows\system32\srvsvc.dll	108 K	
C:\windows\system32\sscore.dll	12 K	
C:\windows\system32\ssdpapi.dll	48 K	
C:\windows\system32\ssdpsrv.dll	284 K	
C:\windows\system32\sspicli.dll	112 K	
C:\windows\system32\sspisrv.dll	24 K	
C:\windows\system32\stdole2.tlb	16 K	
C:\windows\system32\sti_ci.dll	20 K	
C:\windows\system32\stikynot.exe	140 K	
C:\windows\system32\stkhcl32.dll	1 560 K	
C:\windows\system32\stkhtlib.dll	136 K	
C:\windows\system32\stobject.dll	132 K	
handler.dll	12 K	

ОЗУ (на клиентском ПК)

STKHCL32.dll = 1560 K

STKHLIB.dll = 136 K



#нагрузка кейс

Агенты: 3300 шт.

В т.ч. тотальный контроль и мониторинг: 150 агентов

Офис 1



Офис 2



Сервер



База данных

Microsoft SQL server 2014

CPU: 4 ядра, процессор IntelXeon E5645, 2.4Ghz

RAM: 8 Gb

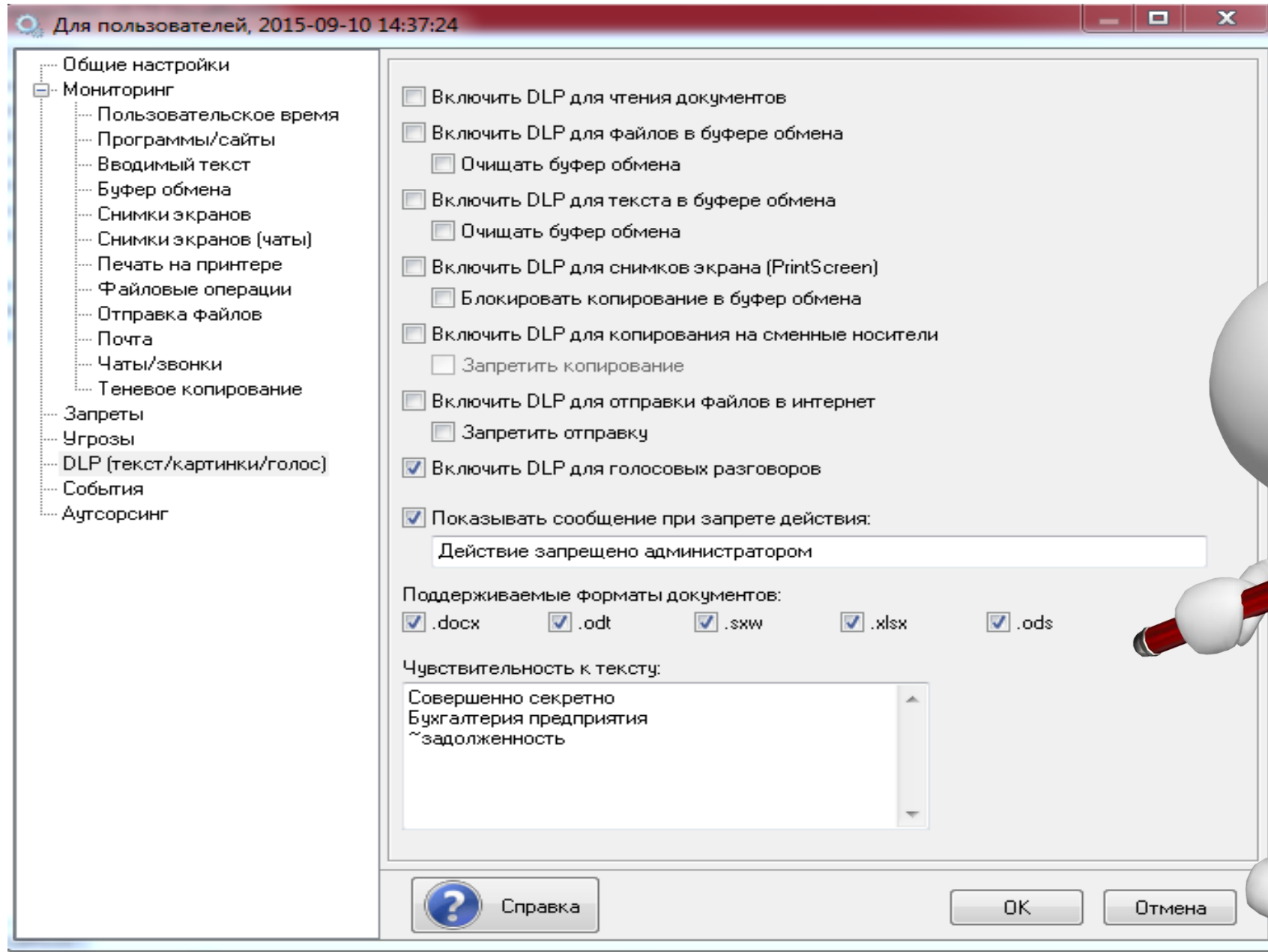
**HDD 1Tb: СХД – VNX5300,
Диски – SAS, ST990080,**

LAN: с высоким приоритетом.

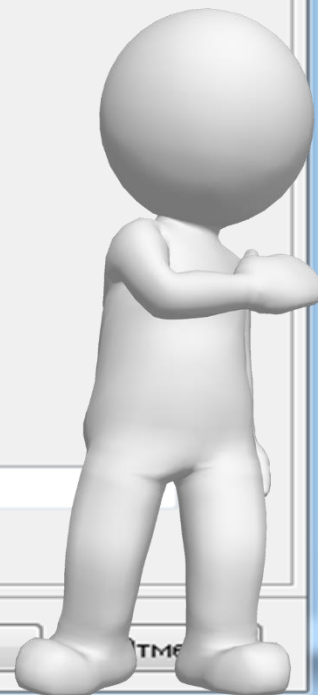
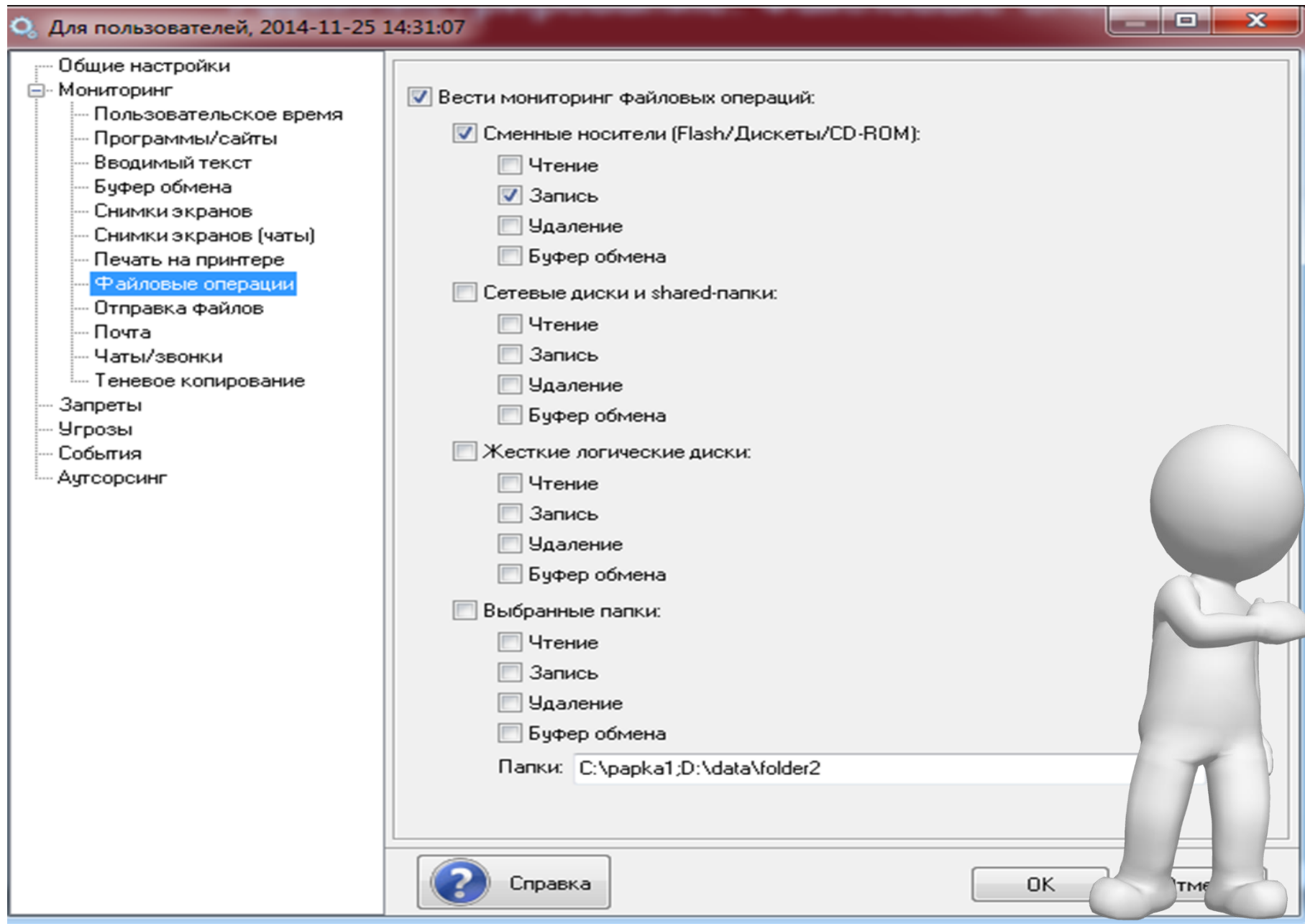
OS: Windows Server 2012 R2



#DLP компонент

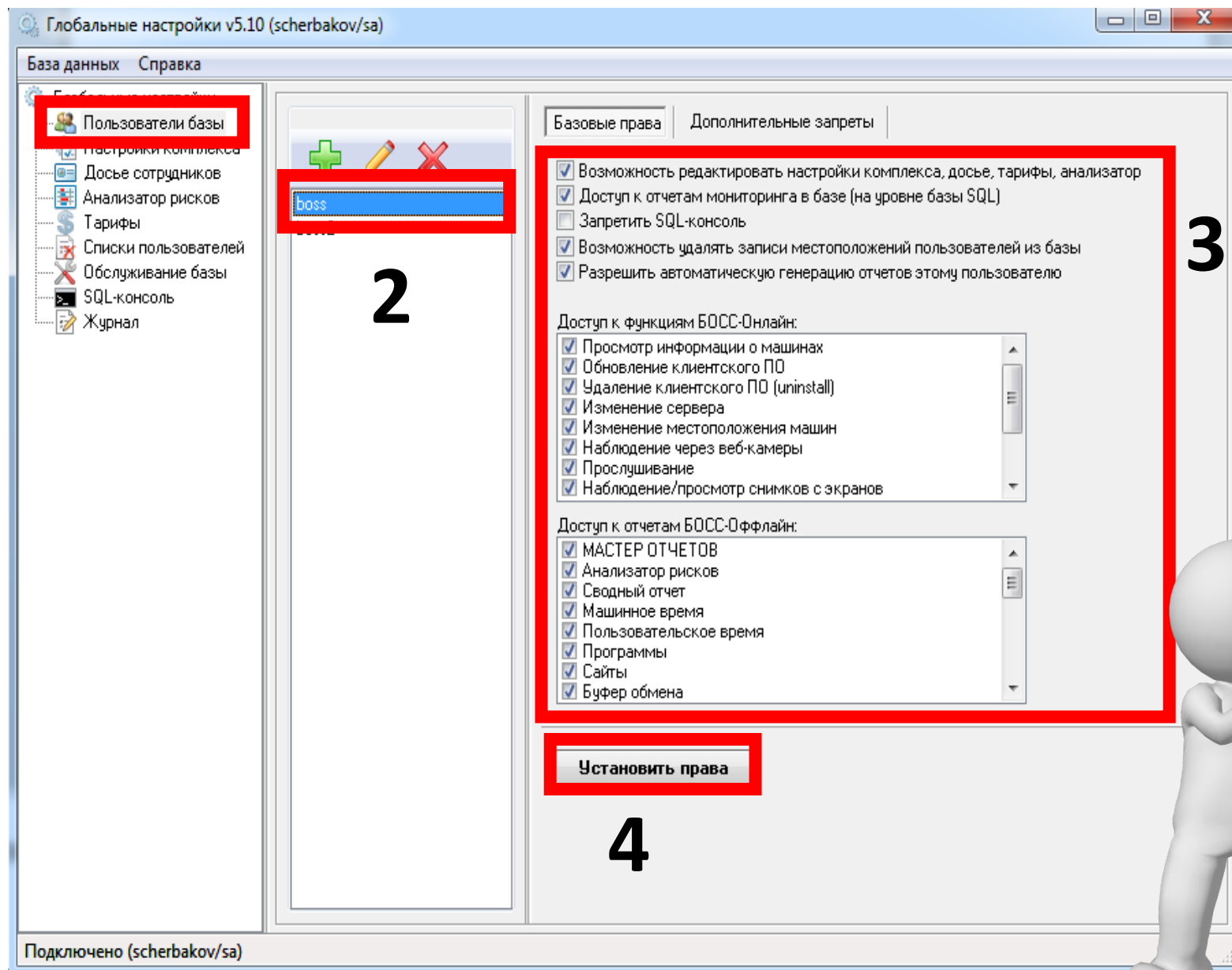


#администрирование #файловые операции



#доступ #права

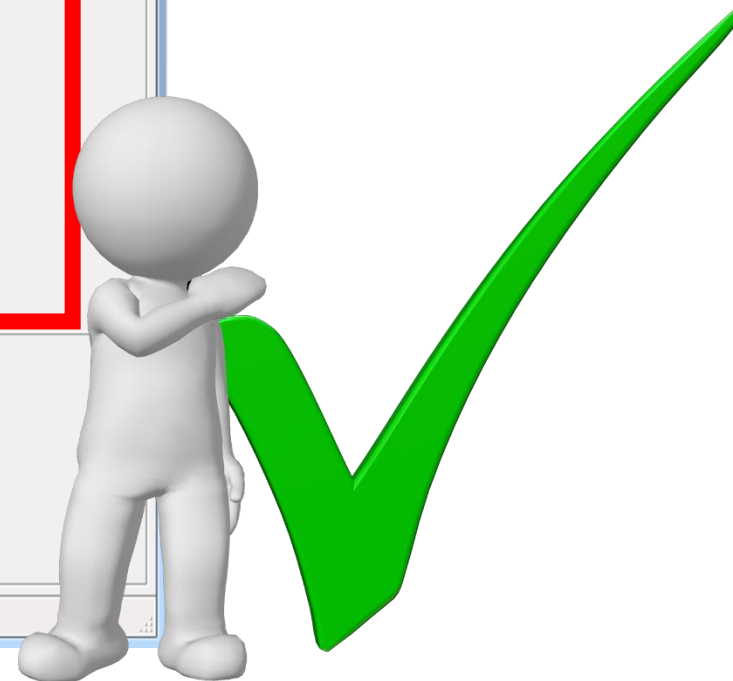
1



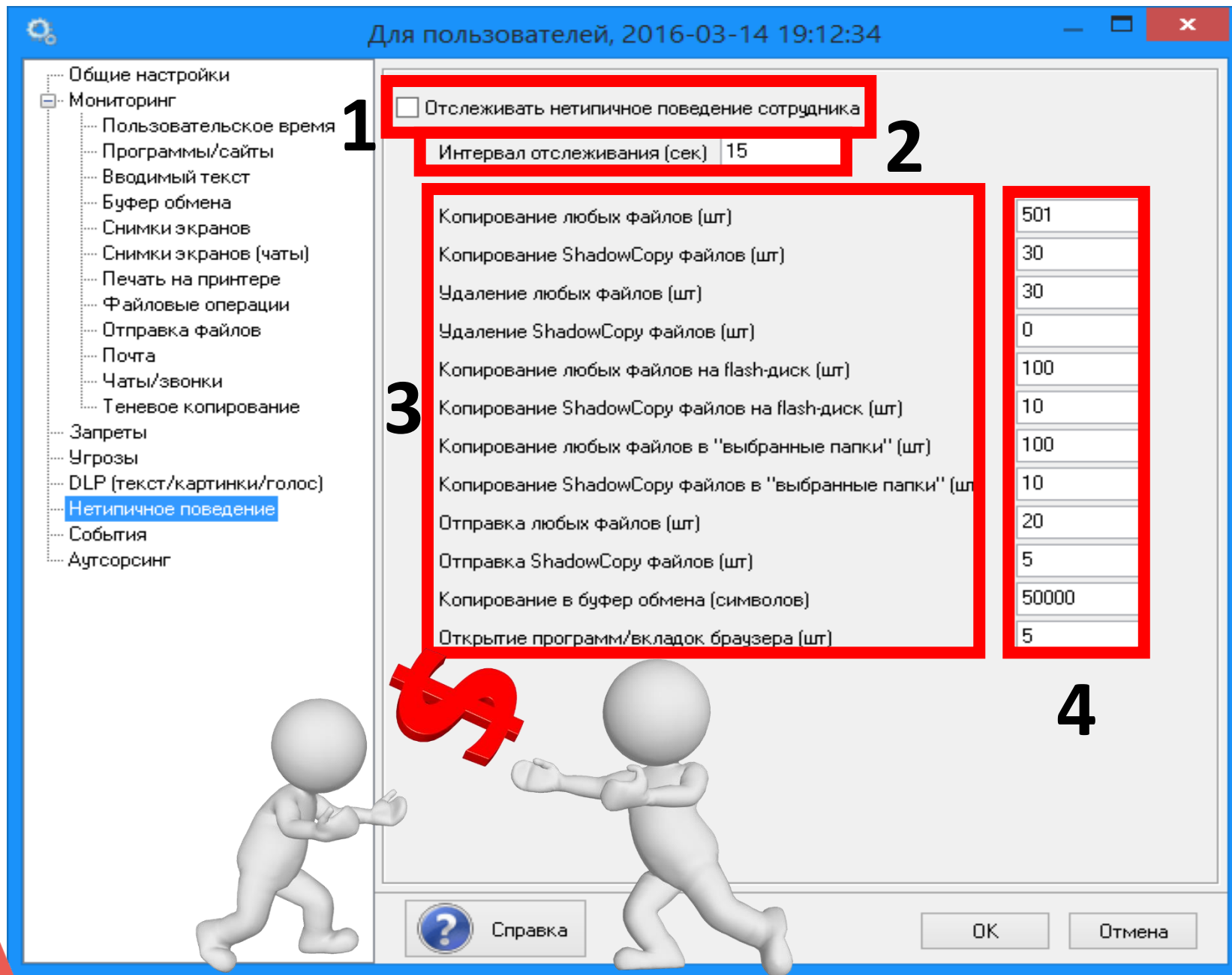
2

3

4



#НЕТИПИЧНОЕ ПОВЕДЕНИЕ



#режимы

Скрытый режим работы

Механизм действия:

Пользователь не получает уведомления о работе пользовательского модуля на компьютере.

Работа программы не отображается в процессах, в панели задач и списке программ, установленных на компьютере.

Плюсы скрытого режима

Позволяет вовремя отследить и предотвратить утечку конфиденциальной информации.

Видимый режим работы

Механизм действия:

При загрузке компьютера пользователь получает сообщение о том, что программа установлена.

Присутствие программы отображается в панели задач и системном трее, запущенных на компьютере.

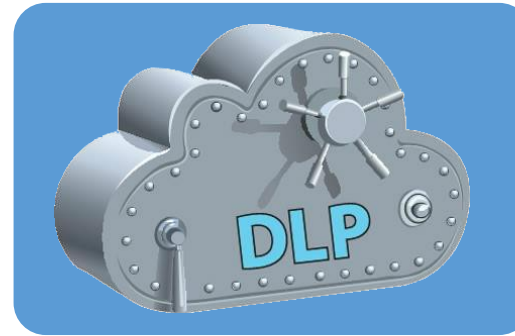
Плюсы видимого режима

Более ответственное отношение сотрудников к рациональному использованию рабочего времени и ресурсов компании.



#интерпретация

KASPERSKY lab  
Проверено! Вирусов НЕТ!



ERP

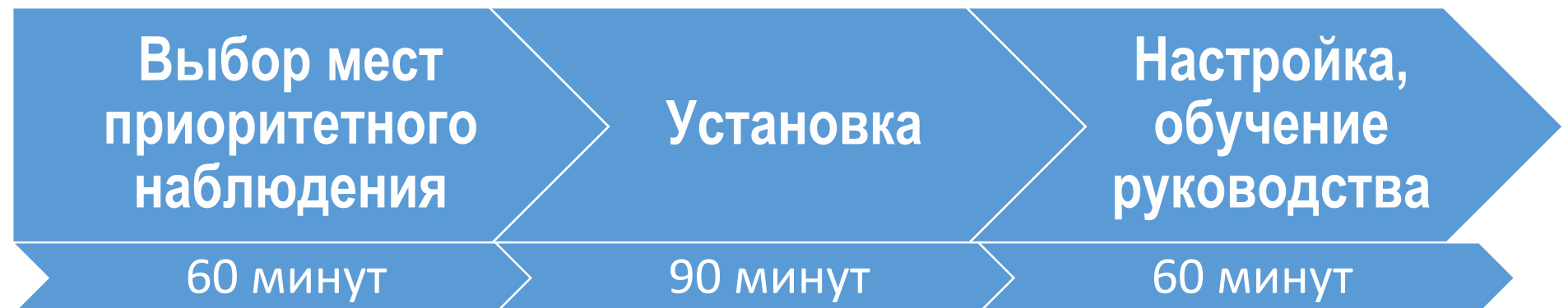
...



#кейсы #real

- Ситуация до внедрения (почему задумались о необходимости такого ПО):
- Уволен коммерческий директор (обнаружились факты продажи своих – конкурирующих услуг клиентам компании), новый только приступил к обязанностям
- Резкое уменьшение заказов от одного из ключевых клиентов, менеджер который его вел не смог объяснить почему
- Увеличение времени на выполнение типовых заказов, что повлекло за собой несвоевременное выполнение работ и стало негативно сказываться на имидже предприятия

Этапы внедрения:



7 дней работы комплекса:

- Выявлены факты грубого, нецензурного общения менеджера с ключевым клиентом (из-за личной неприязни)
- Четыре сотрудника находились в стадии переписки с потенциальными работодателями
- В отделе дизайна менеджеры получив срочную работу в среднем по 4 часа в день тратили на личные нужды. Один из менеджеров 6 часов в день посвящал обучению игре на гитаре, и в конце недели отчитался о невозможности выполнения работы в срок
- Новый коммерческий директор оказался товарищем предыдущего и исправно снабжал его информацией о новых клиентах и ситуации в компании

14 дней работы комплекса:

- Проведена ротация менеджеров, от ключевого клиента поступил первый заказ после продолжительного затишья
- Ряд сотрудников получили дополнительную мотивацию, на места некоторых начали готовить кадровые резервы
- В отделе дизайна менеджеры получили стимулирующее внушение, также была скорректирована система мотивации – уровень дохода поставили в прямую зависимость от «успеваемости» и качества работы
- Новый коммерческий директор был уволен



#лицензирование

- **Лицензируется по количеству устройств**, на которые необходимо установить контроль. **Для терминальных серверов** лицензируется необходимое **количество пользователей сервера**.
- **2 варианта приобретения продукта:**
 - 1) **Пожизненная лицензия** на конкретную мажорную версию продукта (например, на версию 6, которая включает в себя все подверсии 6.XX). Техническая поддержка таким клиентам оказывается до момента прекращения поддержки продукта, но не менее чем 2 года с момента выхода очередной минорной версии.
 - 2) **Временная лицензия** на 1, 2, 3 года. При действующей подписке клиент может перейти на любую стабильную и поддерживаемую версию 6.XX или 7.XX). Техническая поддержка оказывается только при действующей лицензии.
 - 3) **Конкурентный переход.** Подтверждение: копия лицензии конкурирующего продукта или скриншот «О программе» с указанием продукта, юр.лица на которое оформлена лицензия и кол-ва узлов + скан копия Акта приема-передачи прав или Товарной накладной со Счет-фактурой.

Цена в прайсе указана УЖЕ со скидкой за конкурентный переход (см. соответствующие позиции в прайсе и комментарии к ним).

BONUS



#КЛИЕНТЫ

ПРОИЗВОДСТВО ОБОРУДОВАНИЯ

РЕКЛАМНОЕ АГЕНТСТВО

ФИЛИАЛ БАНКА

СУДОРЕМОНТНЫЙ ЗАВОД

ТОРГОВАЯ РОЗНИЧНАЯ СЕТЬ



ФЕДЕРАЛЬНОЕ
ГОСУДАРСТВЕННОЕ
УНИТАРНОЕ
ПРЕДПРИЯТИЕ



Администрация МО
Анапа



ГАЗИНФОРМСЕРВИС



БАНКОРНЕФТЬ



РОСНЕФТЬ



Администрация
города Сургут



УДОБНЫЕ
ДЕНЬГИ



Ростелеком



грузовая
компания



7000 УЗЛОВ



ВОСТРЕБОВАНО! ПОПРОБУЙ...



тел: +7 (495) 272-03-40

dr@stakhanovets.ru



 **Стахановец**