



# Организация в безопасности

**Апостолов Михаил**

**Менеджер по развитию бизнеса**

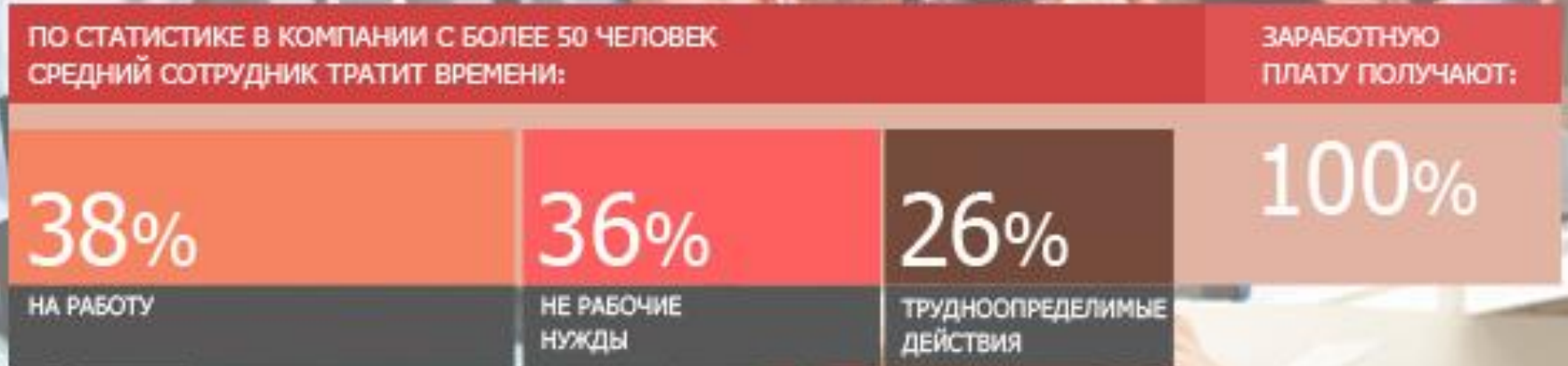
## О чем поговорим:

---

1. Проблемы организаций.
2. Возможности программного комплекса и решаемые им задачи.
3. Структура комплекса.
4. Нагрузка на сеть и ПК.
5. Совместимость со стандартами информационной безопасности.
6. Как использовать Стахановец легально.
7. Бизнес-кейсы.

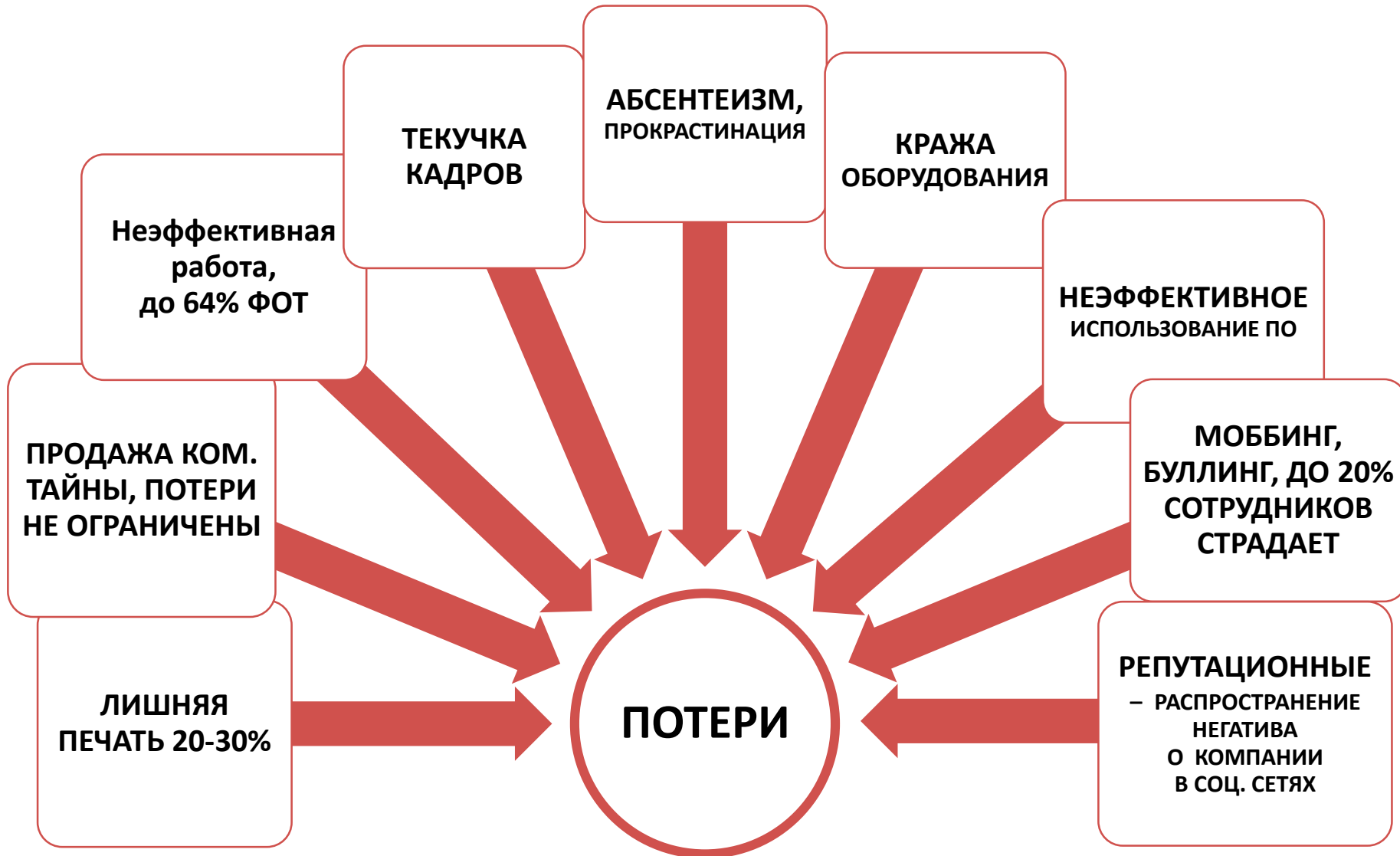


# Проблемы:

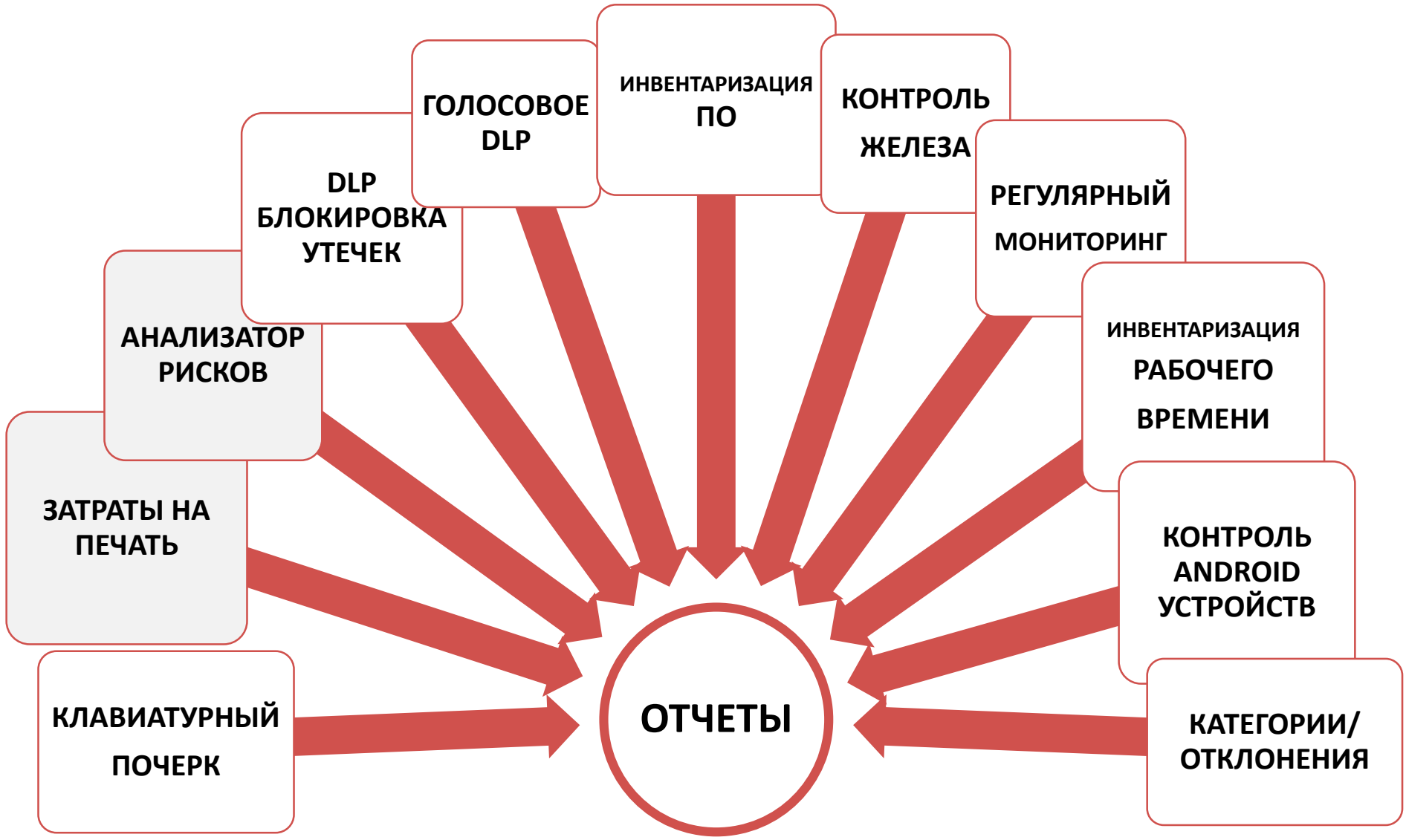


**62%** оплаченного рабочего времени не имеют отношения к работе.  
Средний ущерб от инцидента утечки данных в 2014г составил **\$30млн** для крупных компаний  
Количество «российских» утечек по сравнению с 2013 годом выросло на **73%**

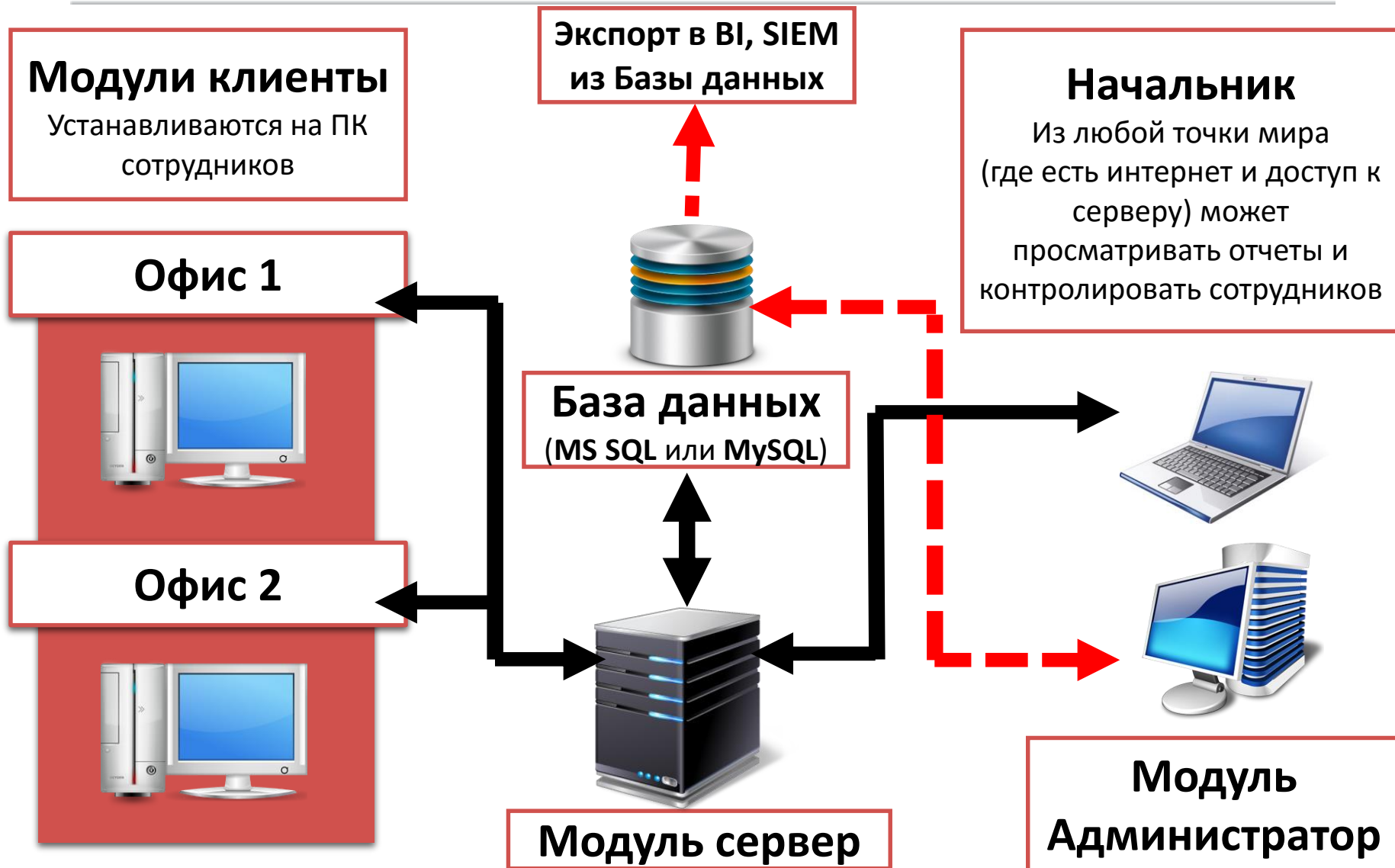
# Проблемы организаций и возможные потери:



# Возможности программного комплекса:



# Структура комплекса:



# Нагрузка на Сеть и ПК:

**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**

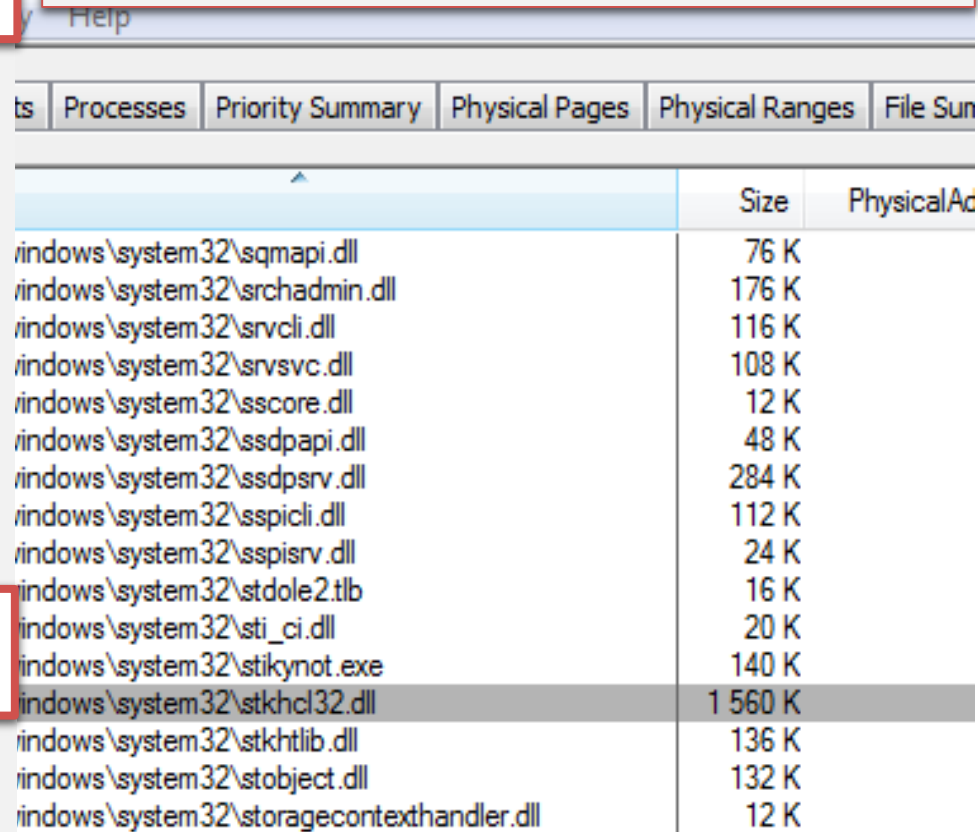
**ОЗУ (на клиентском ПК)**

STKHCL32.dll = **1560 К**

STKHLIB.dll = **136 К**

**НАГРУЗКА НА СЕТЬ**

**Общий мониторинг + скриншоты + видео**



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

## РЕГУЛЯРНЫЙ МОНИТОРИНГ

ПОЛНОТА  
ИНФОРМАЦИИ

ЦЕЛОСТНОСТЬ

ДОСТУПНОСТЬ



*Анализатор  
рисков*



*Принтеры и  
аппаратное  
обеспечение*



*Видео и аудио*



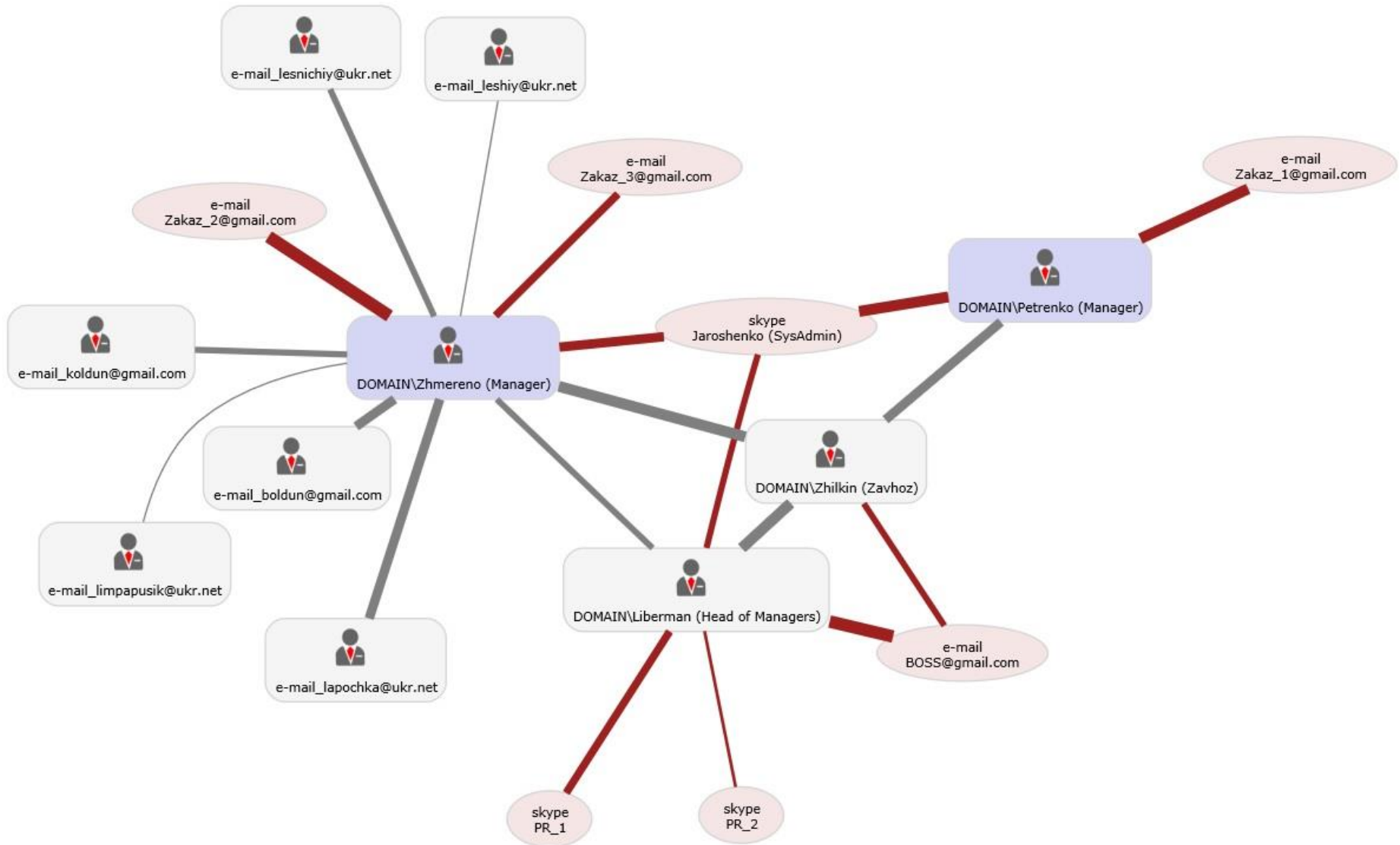
*Сообщения и  
файлы*



*Программы и  
интернет*



# Граф взаимосвязей:



## КЛАВИАТУРНЫЙ ПОЧЕРК

ОЦЕНКА  
СОСТОЯНИЯ  
ПОЛЬЗОВАТЕЛЯ

ИДЕНТИФИКАЦИЯ  
ПОЛЬЗОВАТЕЛЯ

**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)	
	2015-02-02 (ПН)	
	2015-02-03 (BT)	
	2015-02-04 (CP)	



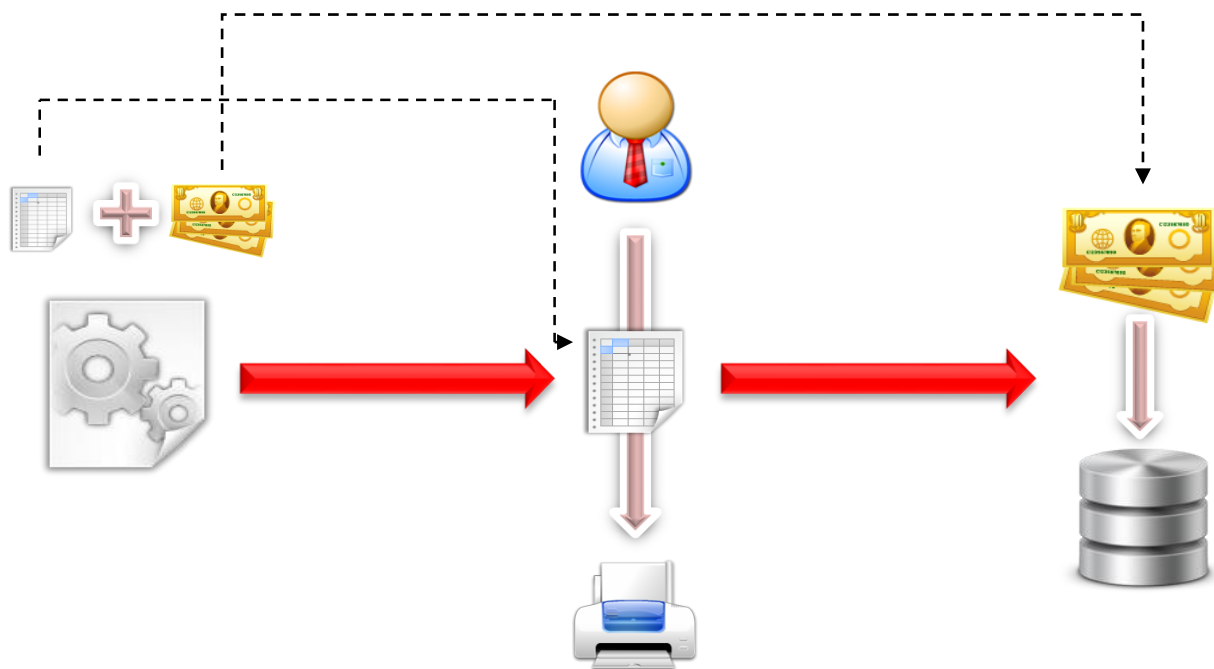
# Затраты на печать:

## ЗАТРАТЫ НА ПЕЧАТЬ

ЦЕЛЕВОЕ  
НАЗНАЧЕНИЕ  
ПЕЧАТИ

КОНТРОЛЬ И  
ОПТИМИЗАЦИЯ  
ЗАТРАТ НА ПЕЧАТЬ

Пользователь	Время	Страниц	КБайт	Бумага	Цвет	Документ	При
LAPTOP\Sergey (Годунов С.В.) Всего страниц: <b>12</b> Стоимость: <b>30,00</b>	2015-01-20 10:19	4	64 КБ	A4 210x297	Цвет	<i>Безымянный – Блокнот</i> <a href="#">2015-01-20 10-19-17 00002.spl</a> <a href="#">2015-01-20 10-19-17 00002.shd</a>	HP Deskjet
	2015-01-20 10:26	4	64 КБ	A4 210x297	Цвет	<i>Безымянный – Блокнот</i> <a href="#">2015-01-20 10-26-20 00003.spl</a> <a href="#">2015-01-20 10-26-20 00003.shd</a>	HP Deskjet
	2015-01-20 10:36	4	64 КБ	A4 210x297	Цвет	<i>Безымянный – Блокнот</i> <a href="#">2015-01-20 10-36-47 00004.spl</a> <a href="#">2015-01-20 10-36-47 00004.shd</a>	HP Deskjet



# Анализатор рисков:

## АНАЛИЗАТОР РИСКОВ

АВТОМАТИЧЕСКАЯ  
КЛАССИФИКАЦИЯ  
АКТИВНОСТИ  
ПОЛЬЗОВАТЕЛЕЙ

ПРОФИЛИ  
СОТРУДНИКОВ

ОБНАРУЖЕНИЕ  
КАДРОВЫХ И  
ИНФОРМАЦИОННЫХ  
РИСКОВ

Пользователь	Социальные сети	СМИ и развлечения	Поиск работы	Возможный вред	Рабочие
erg-ПК\erg (долинская е.и) отдел: бух профиль: По умолчанию	2ч37м 22%	0ч02м 1%	0ч00м <b>6</b>	0ч00м 0%	0ч55м 8%

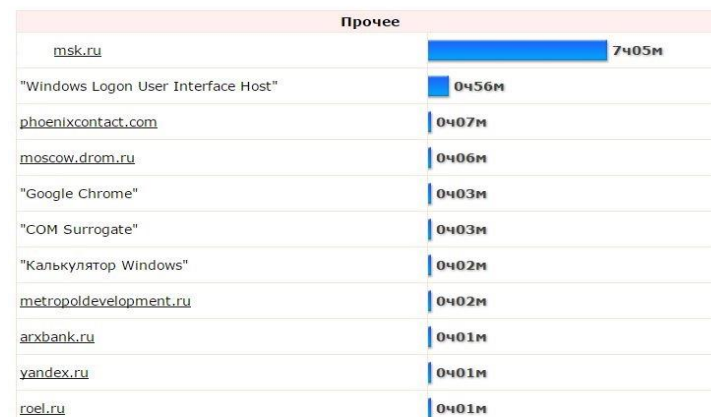
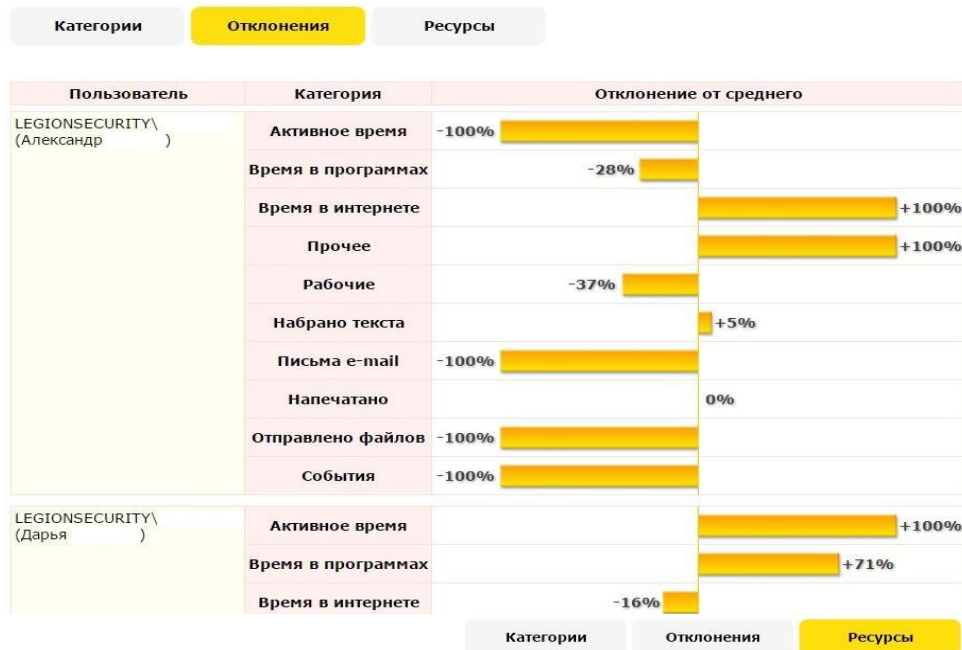
Пользователь	Социальные сети	СМИ и развлечения	Поиск работы	Возможный вред	Рабочие	Прочее
erg-ПК\erg (долинская е.и) отдел: бух профиль: По умолчанию	2ч37м 22% vk.com (22%, 2ч37м)	0ч02м 1% ivi.ru (1%, 0ч02м)	0ч00м 0% <b>6</b> ~работа (6)	0ч00м 0%	0ч55м 8% "Adobe Reader 9.0" (5%, 0ч30м) "Microsoft Office Word" (3%, 0ч19) "Проводник" (1%, 0ч07м)	2ч49м 24%

## КАТЕГОРИИ / ОТКЛОНЕНИЯ

ПОВЕДЕНИЕ УСПЕШНЫХ СОТРУДНИКОВ И ТРАНСЛЯЦИЯ ПОКАЗАТЕЛЕЙ НА ОСТАЛЬНОЙ ПЕРСОНАЛ

ПОВЕДЕНИЕ СОТРУДНИКОВ, С НИЗКОЙ ПРОИЗВОДИТЕЛЬНОСТЬЮ. ВЫЯВЛЕНИЕ ПОМЕХ И ОПРЕДЕЛЕНИЕ НЕЭФФЕКТИВНЫХ МОДЕЛЕЙ РАБОТЫ

ПОИСК ОТКЛОНЕНИЙ В ПОВЕДЕНИИ ДЛЯ ОПРЕДЕЛЕНИЯ ИНСАЙДЕРОВ, РИСКОВЫХ КАТЕГОРИЙ И НЕЛОЯЛЬНОГО ПЕРСОНАЛА

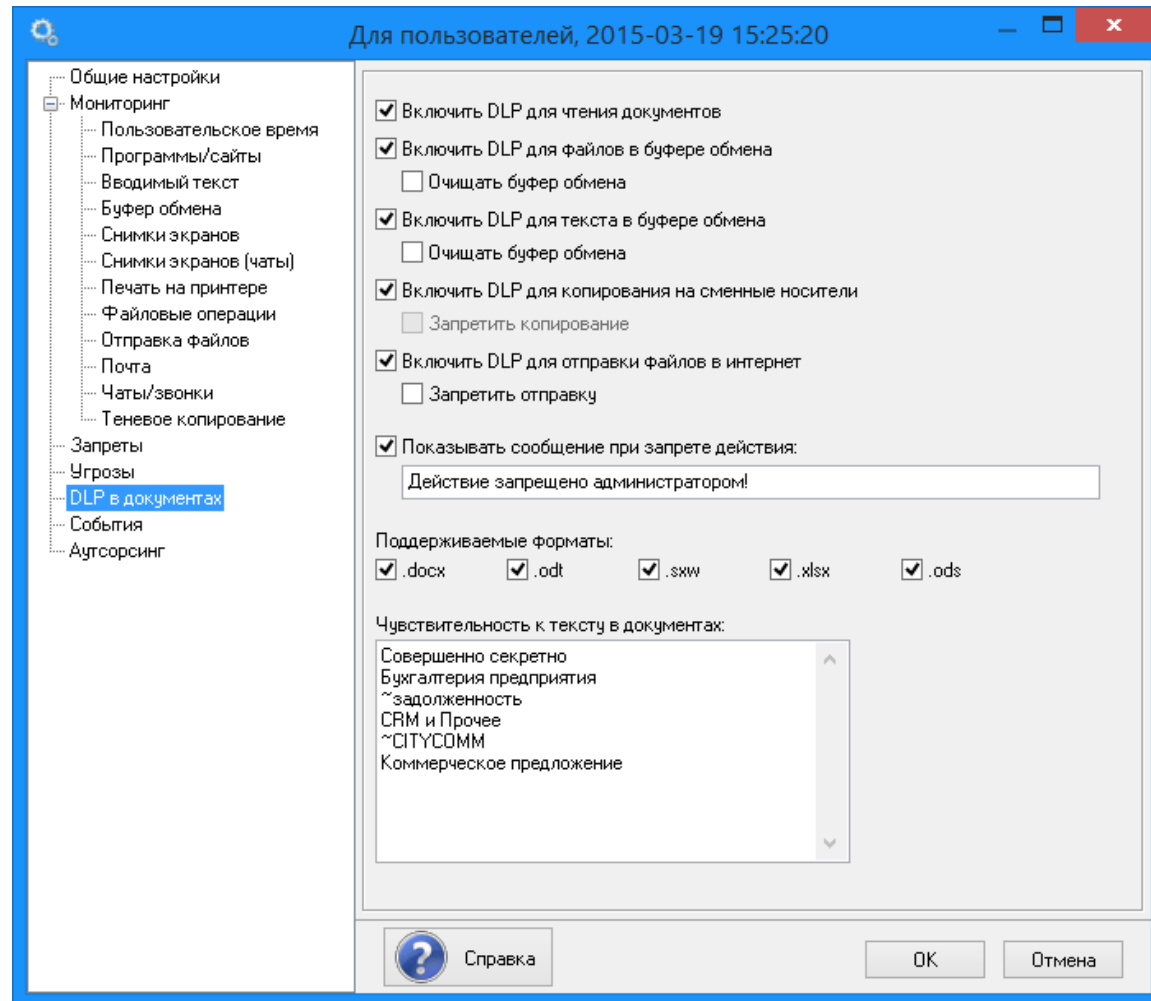


# Предотвращение утечек информации:

**DLP В ДОКУМЕНТАХ**  
(открытие, копирование,  
вывод в интернет, буфер  
обмена) по ключевым  
словам/фразам

**ПОДДЕРЖИВАЕТСЯ  
ПОЛНОТЕКСТОВЫЙ  
НЕЧЕТКИЙ ПОИСК**

**ВЫСОКАЯ  
ПРОИЗВОДИТЕЛЬНОСТЬ И  
НИЗКОЕ ПОТРЕБЛЕНИЕ РЕСУРСОВ  
НА ТОНКИХ КЛИЕНТАХ**



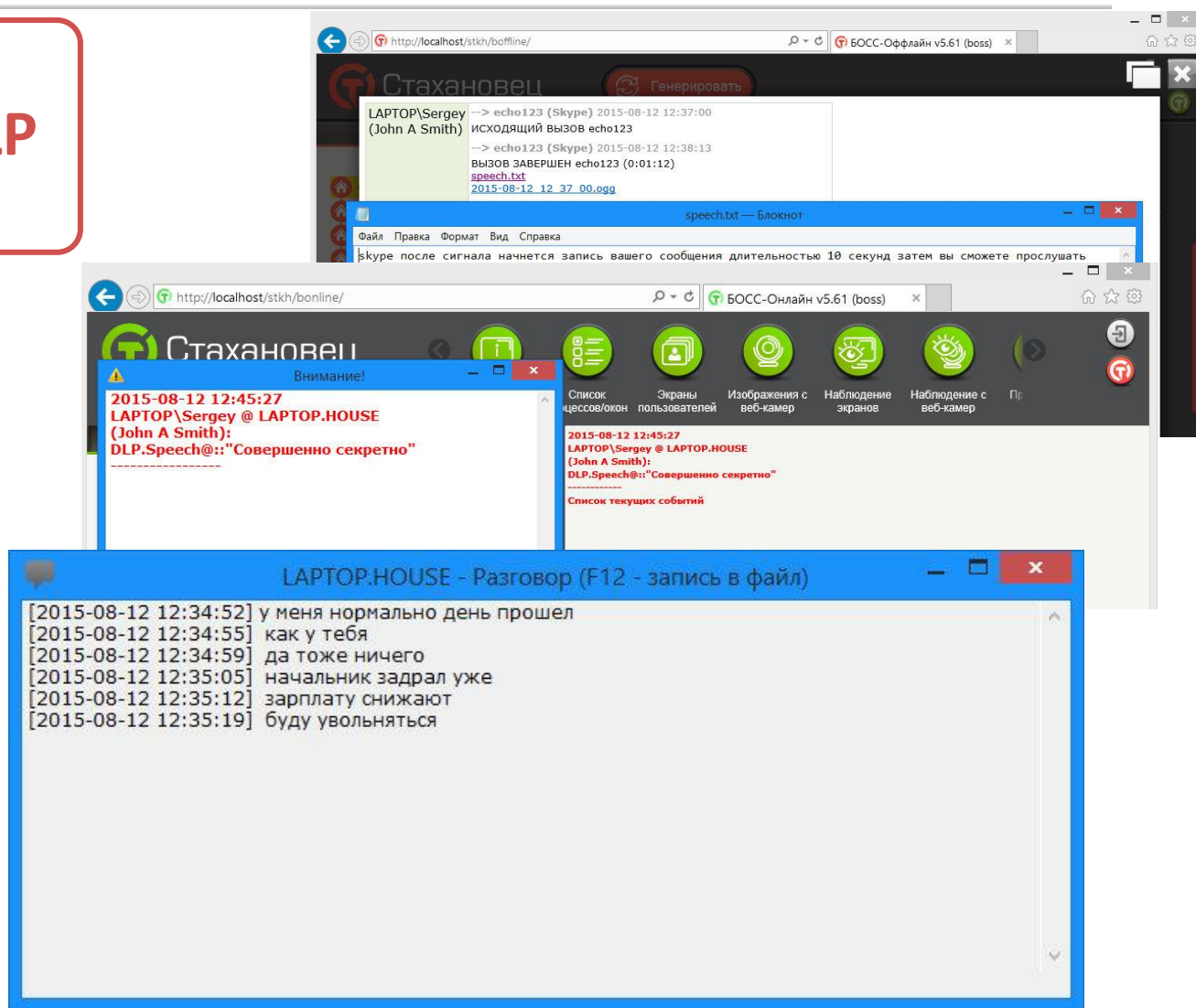
# Предотвращение утечек информации:

## ГОЛОСОВОЕ DLP

РЕАКЦИЯ НА «КОДОВУЮ  
ФРАЗУ» И МГНОВЕННОЕ  
УВЕДОМЛЕНИЕ СЛУЖБЫ  
БЕЗОПАСНОСТИ

ФИКСАЦИЯ И  
РАСПОЗНАВАНИЕ  
ДИАЛОГОВ В РАЗЛИЧНЫХ  
МЕССЕНЖЕРАХ:  
Skype, Lync, Viber

ПРОСЛУШИВАНИЕ  
ПЕРЕГОВОРОВ В РЕЖИМЕ  
РЕАЛЬНОГО ВРЕМЕНИ



The screenshot displays the Stokhanovets software interface with several windows open:

- BOSS-Оффлайн v5.61 (boss)**: A window showing a log of voice calls. It includes a "Генерировать" button and a list of events such as "исходящий вызов echo123" and "Вызов ЗАВЕРШЕН echo123 (0:01:12)". A "speech.txt" file is mentioned with a timestamp of "2015-08-12 12 37 00.ogg".
- speech.txt — Блокнот**: A Notepad window with a message: "skype после сигнала начнется запись вашего сообщения длительностью 10 секунд затем вы сможете прослушать".
- BOSS-Онлайн v5.61 (boss)**: A window showing a "Внимание!" (Attention!) alert. The alert text reads: "2015-08-12 12:45:27 LAPTOP\Sergey @ LAPTOP.HOUSE (John A Smith): DLP.Speech@: 'Совершенно секретно'". Below the alert, there are icons for "Список часов/окон", "Экраны пользователей", "Изображения с веб-камер", "Наблюдение экранов", and "Наблюдение с веб-камер".
- LAPTOP.HOUSE - Разговор (F12 - запись в файл)**: A window showing a real-time transcript of a conversation. The text includes: "[2015-08-12 12:34:52] у меня нормально день прошел", "[2015-08-12 12:34:55] как у тебя", "[2015-08-12 12:34:59] да тоже ничего", "[2015-08-12 12:35:05] начальник задрал уже", "[2015-08-12 12:35:12] зарплату снижают", and "[2015-08-12 12:35:19] буду увольняться".

## КОНТРОЛЬ ЖЕЛЕЗА

СКОЛЬКО КАКИХ  
АППАРАТНЫХ  
КОМПОНЕНТ  
УСТАНОВЛЕНО И ГДЕ

ОПОВЕЩЕНИЕ О  
ИЗМЕНЕНИЯХ

```
LAPTOP.HOUSE [2015-02-03] Процессор {
Description = "Intel64 Family 6 Model 58 Stepping 9"
Caption = "Intel64 Family 6 Model 58 Stepping 9"
Name = "Intel(R) Core(TM) i5-3317U CPU @ 1.70GHz"
Manufacturer = "GenuineIntel"
DeviceID = "CPU0"
MaxClockSpeed = "1700"
NumberOfCores = "2"
NumberOfLogicalProcessors = "4"
ProcessorId = "BFEBFBFF000306A9"
SocketDesignation = "SOCKET 0"
Version = ""
};

[2015-02-03] Материнская плата {
Description = "Основная плата"
Caption = "Основная плата"
Name = "Основная плата"
Manufacturer = "ASUSTeK COMPUTER INC."
Product = "P500CA"
SerialNumber = "BSN12345678901234567"
};

[2015-02-03] BIOS {
Description = "P500CA.208"
Caption = "P500CA.208"
Name = "P500CA.208"
Manufacturer = "American Megatrends Inc."
SerialNumber = "D5NXCY090144187 "
SMBIOSBIOSVersion = "P500CA.208"
SoftwareElementID = "P500CA.208"
Version = "_ASUS_ - 1072009"
};
```

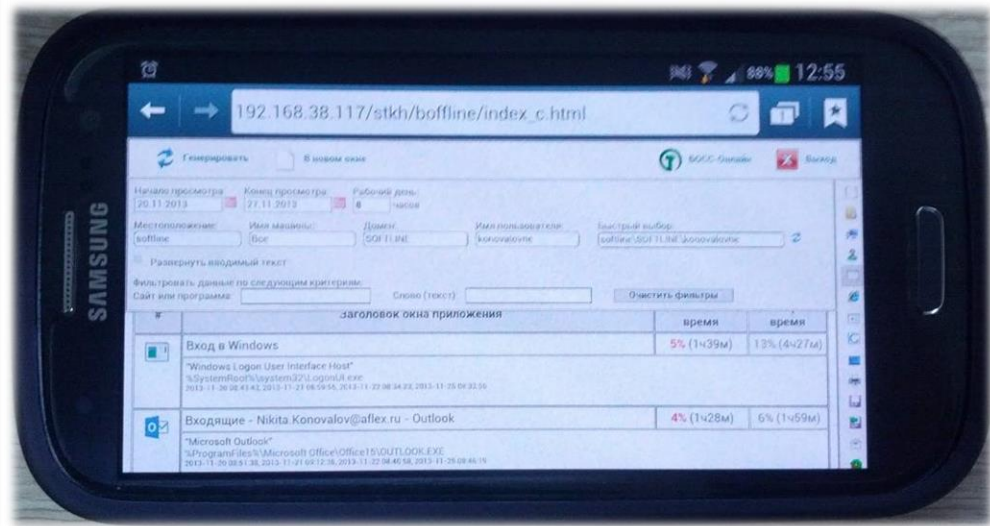
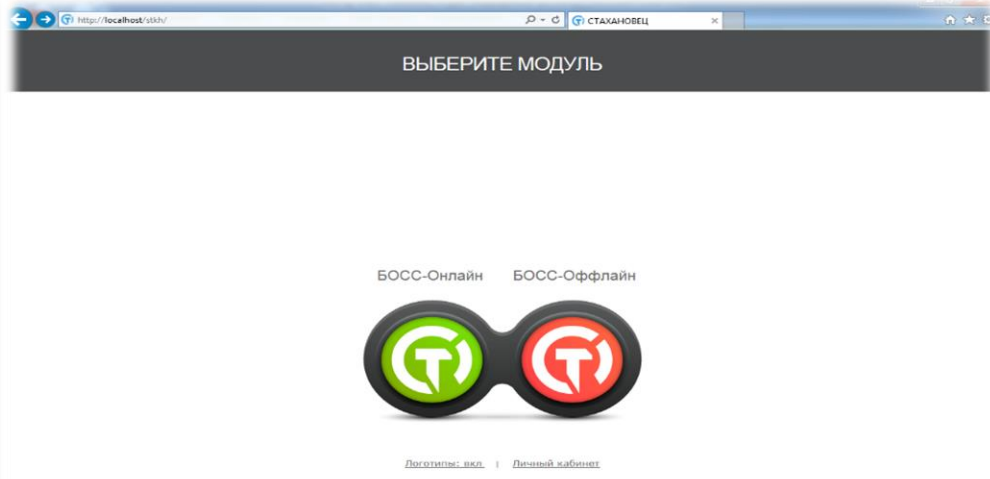
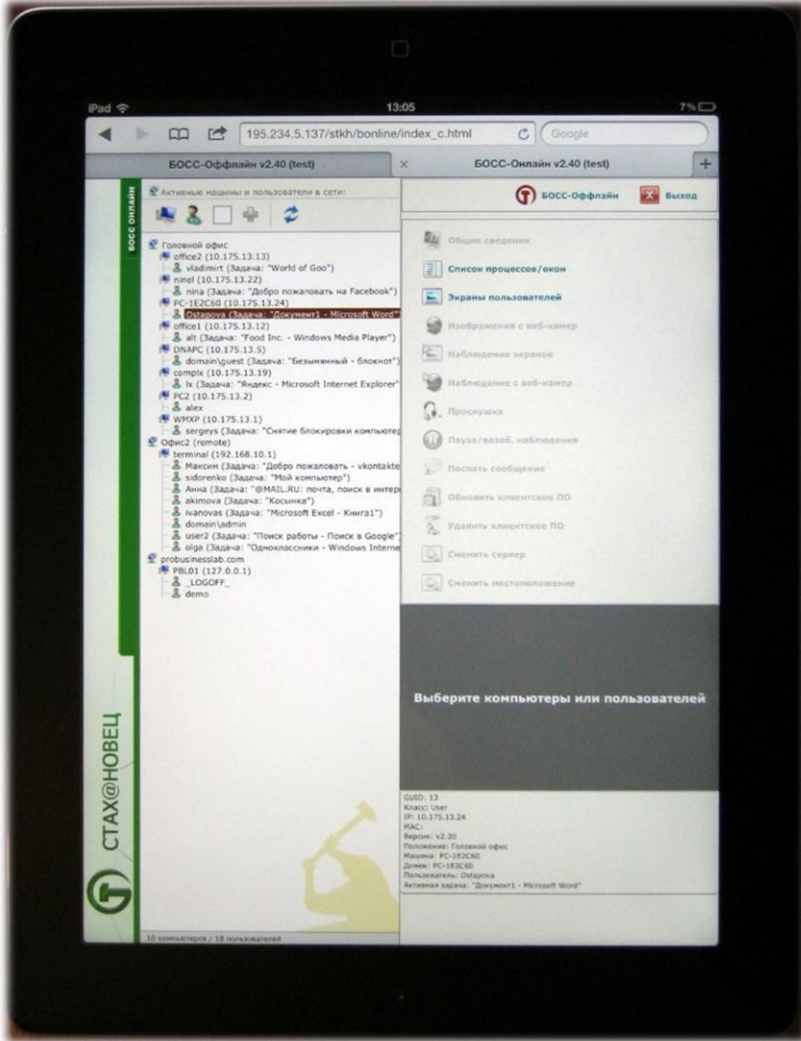


## ИНВЕНТАРИЗАЦИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

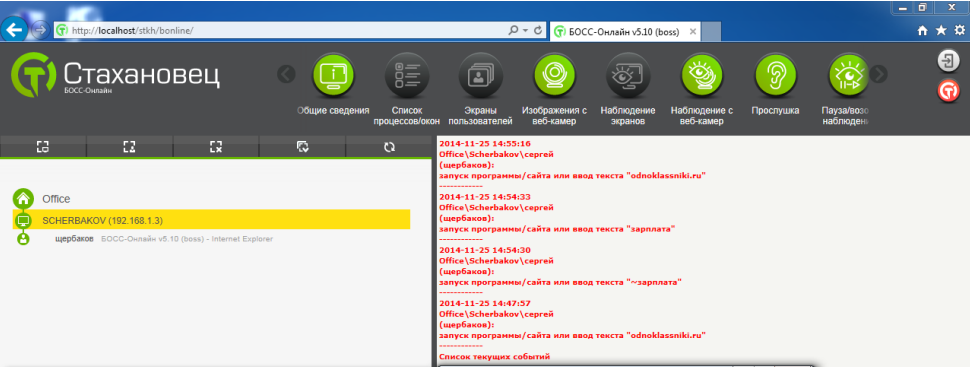
СКОЛЬКО КАКИХ  
ПРОГРАММНЫХ  
ПРОДУКТОВ  
УСТАВЛЕНО И ГДЕ

Программа	Кол-во установок	Компьютеры
Avast Free Antivirus	1	<a href="#">показать список</a>
Bandizip	1	<a href="#">показать список</a>
CrystalDiskInfo 6.2.2	1	<a href="#">показать список</a>
Definition Update for Microsoft Office 2010 (KB2956079) 32-Bit Edition	1	<a href="#">показать список</a>
Energy Management	1	<a href="#">показать список</a>
EPSON Scan	1	<a href="#">показать список</a>
EPSON XP-312 313 315 Series Printer Uninstall	1	<a href="#">показать список</a>
EpsonNet Print	1	<a href="#">показать список</a>
Free Media Opener 1.0	1	<a href="#">показать список</a>
Google Chrome	1	<a href="#">показать список</a>
Google Toolbar for Internet Explorer	1	<a href="#">показать список</a>
Google Update Helper	1	<a href="#">показать список</a>
Java 8 Update 25	1	<a href="#">показать список</a>
Java Auto Updater	1	<a href="#">показать список</a>
Lenovo EasyCamera	1	<a href="#">показать список</a>
Microsoft Application Error Reporting	1	<a href="#">показать список</a>
Microsoft Office Access MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Excel MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Groove MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office InfoPath MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Office 64-bit Components 2010	1	<a href="#">показать список</a>
Microsoft Office OneNote MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Outlook MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office PowerPoint MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Professional Plus 2010	1	<a href="#">показать список</a>
Microsoft Office Proof (English) 2010	1	<a href="#">показать список</a>
Microsoft Office Proof (German) 2010	1	<a href="#">показать список</a>
Microsoft Office Proof (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Proof (Ukrainian) 2010	1	<a href="#">показать список</a>
Microsoft Office Proofing (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Publisher MUI (Russian) 2010	1	<a href="#">показать список</a>
Microsoft Office Shared 64-bit MUI (Russian) 2010	1	<a href="#">показать список</a>

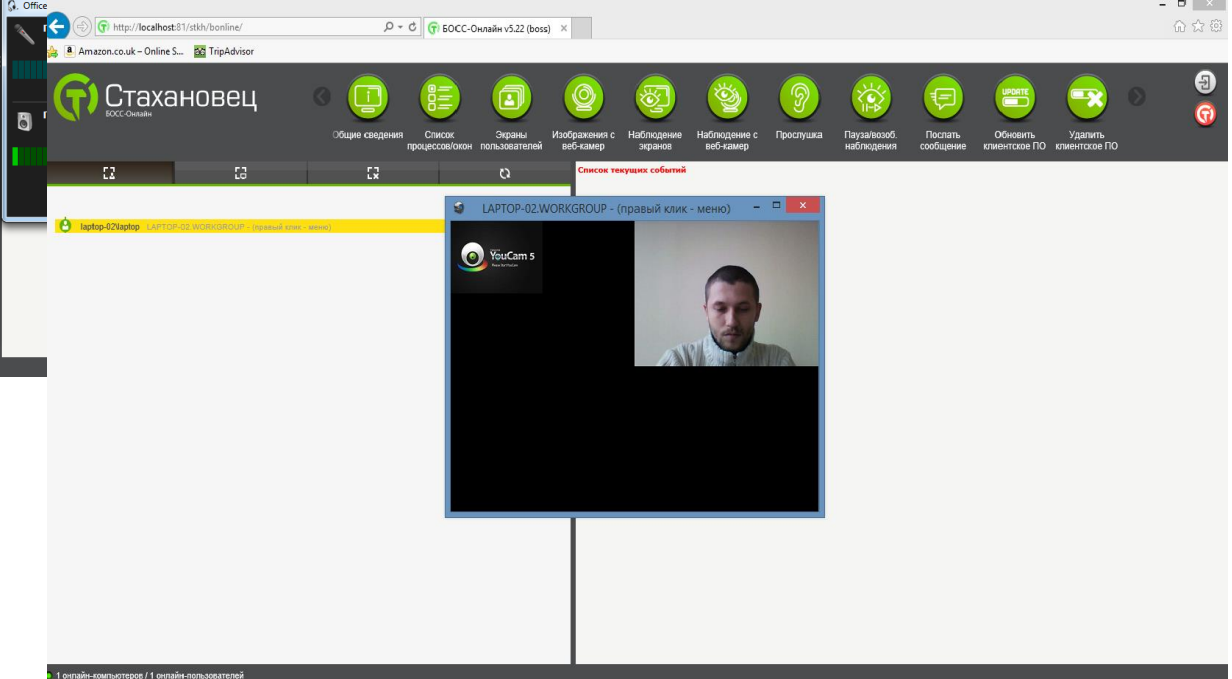
# Работа на смартфонах и планшетах:



# Модуль БОСС – Онлайн Веб-камера и звук:



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"  
-----  
2014-11-25 14:47:57  
Office (Scherbakov)\сергей (щербakov):  
запуск программы/сайта или ввод текста "odnoklassniki.ru"  
-----  
Список текущих событий

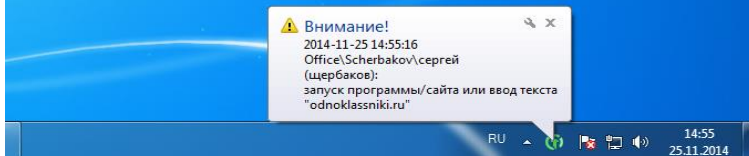
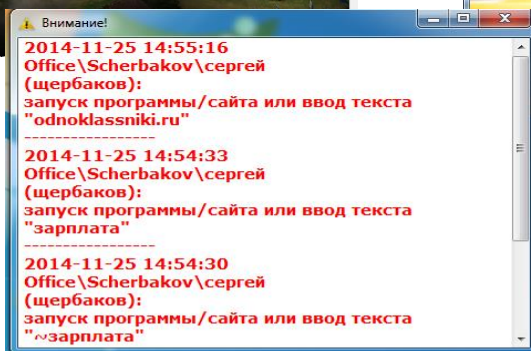
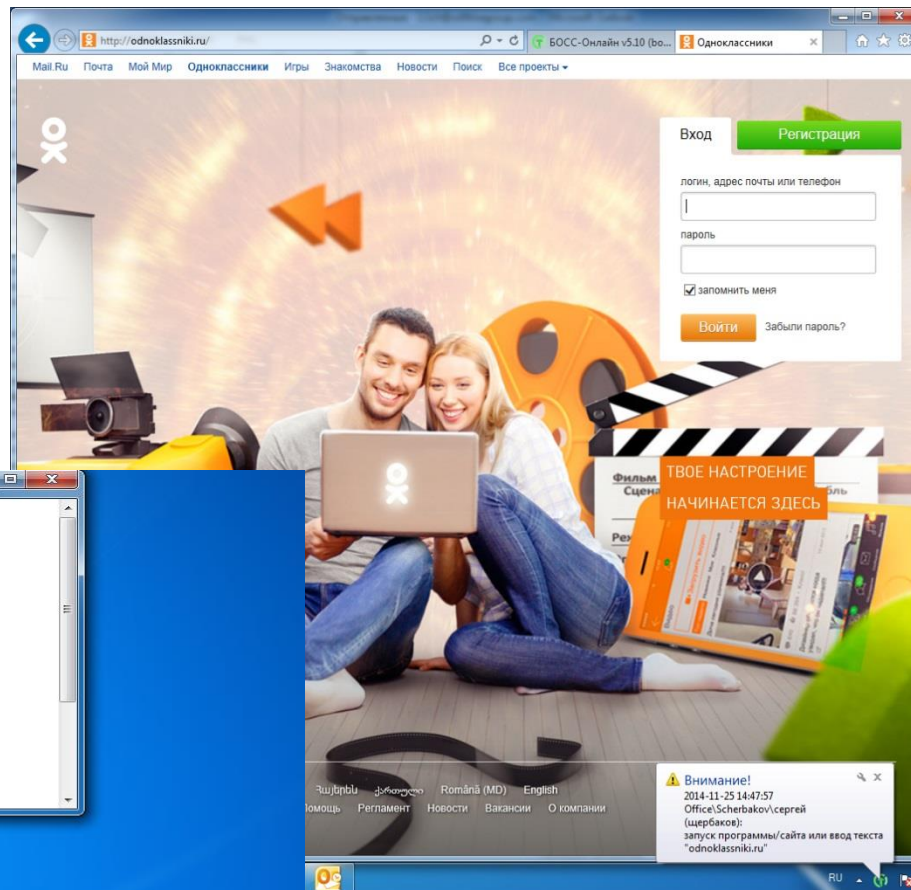
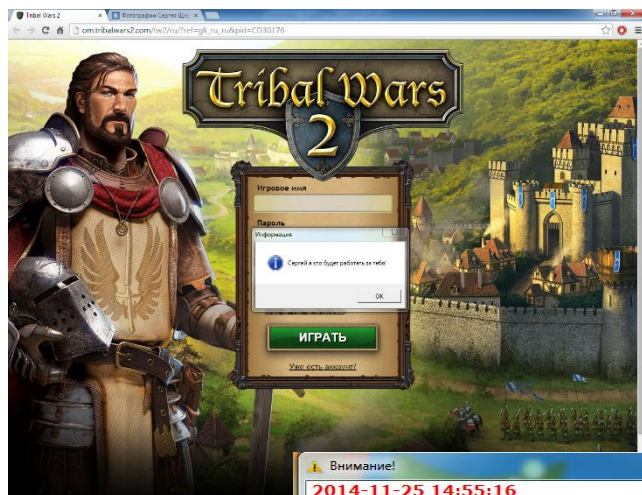


Список текущих событий

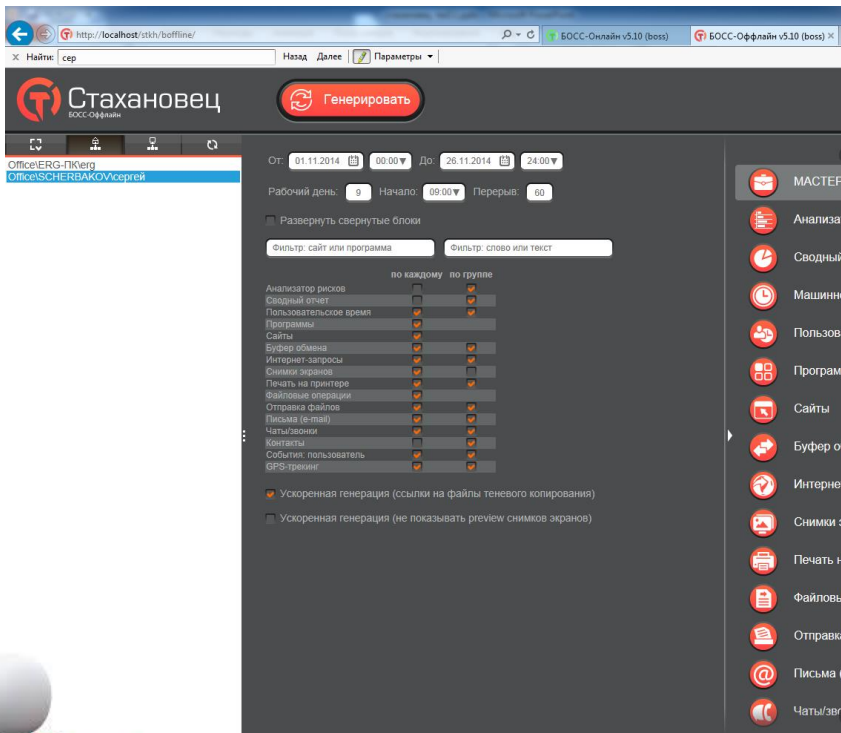
1 онлайн-компьютеров / 1 онлайн-пользователей



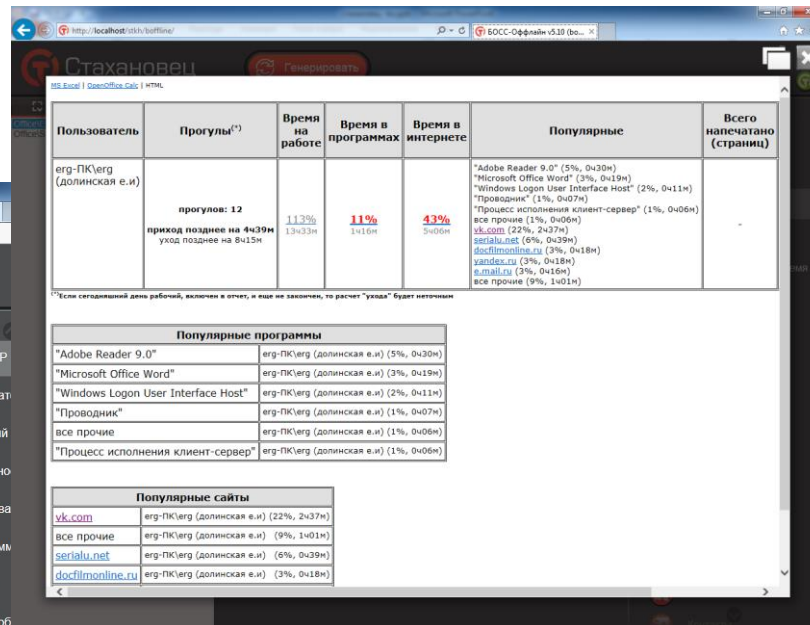
# Модуль БОСС – Онлайн Отправка сообщения:



# Модуль БОСС – Офлайн:



Скриншот интерфейса модуля БОСС – Офлайн. Вверху отображены кнопки "Назад", "Далее" и "Параметры". В центре — панель "Генерировать" с датой отбора: 01.11.2014 до 26.11.2014. Слева — список пользователей: Office:ERG-ПКerg, Office:SCHEERBAKOV\corp\rey. Справа — панель настроек отчета с чек-боксами для различных категорий данных.



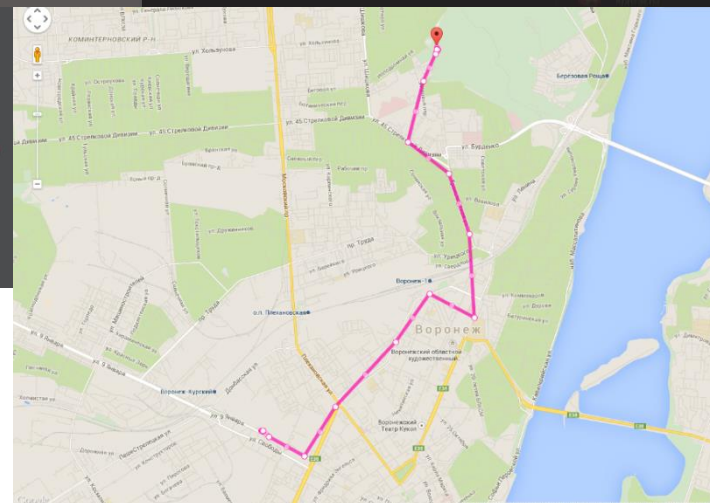
Скриншот интерфейса модуля БОСС – Офлайн, отображающий отчет по пользователю erg-ПК\erg (должностная единица).

Пользователь	Прогулы <sup>(*)</sup>	Время на работе	Время в программах	Время в интернете	Популярные	Всего напечатано (страниц)
erg-ПК\erg (должностная е.и)	прогулов: 12 приход позднее на 4ч39м уход позднее на 8ч15м	113% 13ч43м	11% 1ч11м	43% 2ч04м	"Adobe Reader 9.0" (5%, 0ч20м) "Microsoft Office Word" (3%, 0ч19м) "Windows Logon User Interface Host" (2%, 0ч11м) "Проводник" (1%, 0ч07м) "Процесс исполнения клиент-сервер" (1%, 0ч06м) все прочие (1%, 0ч06м) vk.com (22%, 2ч37м) serialu.net (6%, 0ч39м) docfilmonline.ru (3%, 0ч18м) karsk.ru (3%, 0ч18м) e.mail.ru (3%, 0ч16м) все прочие (9%, 1ч01м)	

\*Если сегодняшний день рабочий, включен в отчет, и еще не закончен, то расчет "ухода" будет неточным

Популярные программы	
"Adobe Reader 9.0"	erg-ПК\erg (должностная е.и) (5%, 0ч20м)
"Microsoft Office Word"	erg-ПК\erg (должностная е.и) (3%, 0ч19м)
"Windows Logon User Interface Host"	erg-ПК\erg (должностная е.и) (2%, 0ч11м)
"Проводник"	erg-ПК\erg (должностная е.и) (1%, 0ч07м)
все прочие	erg-ПК\erg (должностная е.и) (1%, 0ч06м)
"Процесс исполнения клиент-сервер"	erg-ПК\erg (должностная е.и) (1%, 0ч06м)

Популярные сайты	
vk.com	erg-ПК\erg (должностная е.и) (22%, 2ч37м)
все прочие	erg-ПК\erg (должностная е.и) (9%, 1ч01м)
serialu.net	erg-ПК\erg (должностная е.и) (6%, 0ч39м)
docfilmonline.ru	erg-ПК\erg (должностная е.и) (3%, 0ч18м)



## 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.

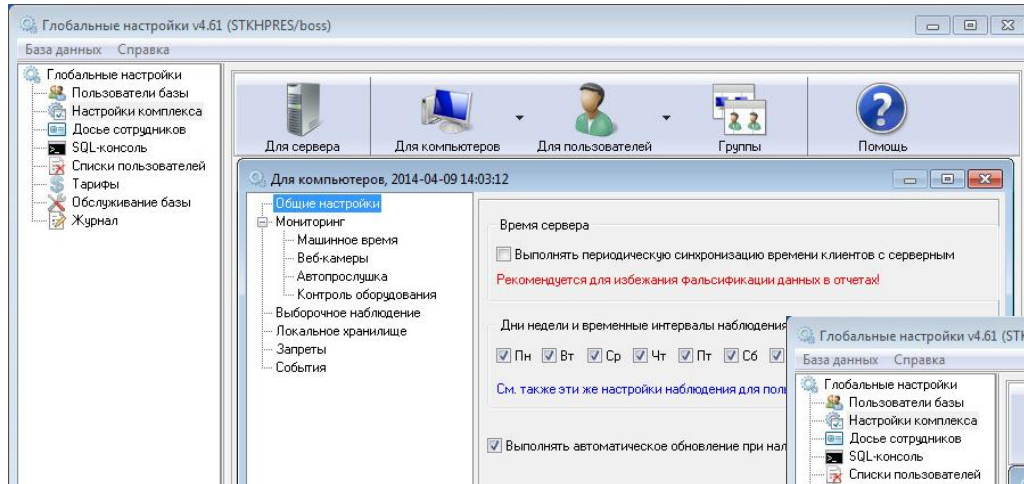
### Плюсы видимого режима:

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

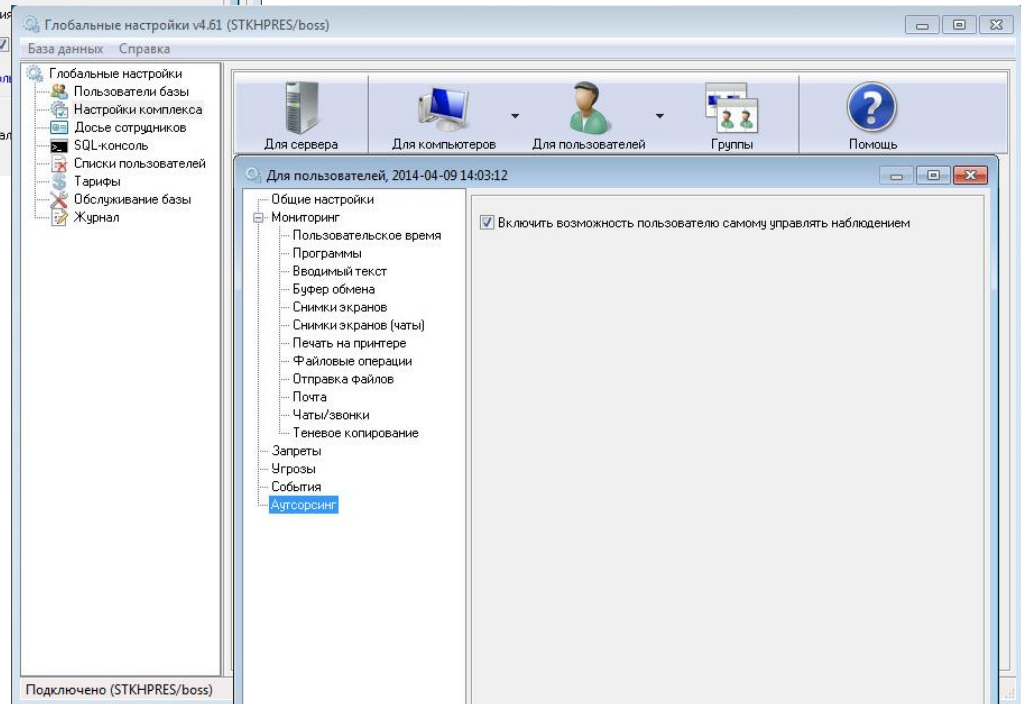


# Режимы работы:

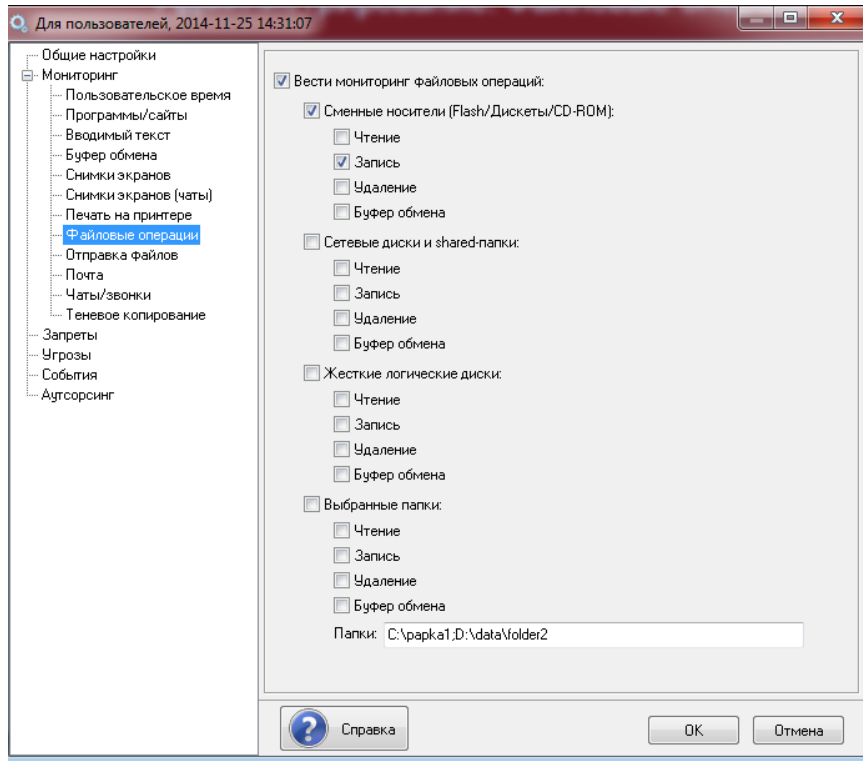
## Можно выбирать время наблюдения



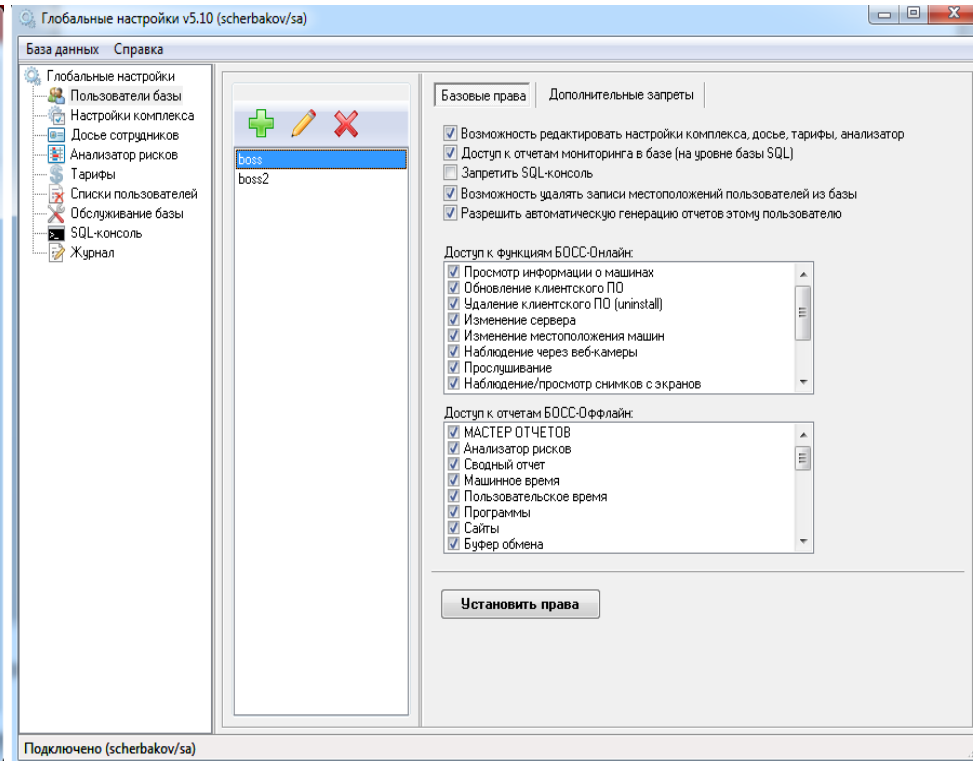
**Сотрудник может сам  
включать и выключать  
наблюдение**



## Файловые операции



## Каждому свои права





# Совместимость со стандартами ИБ:



**СОВМЕСТИМОСТЬ**

**ПОМОЩЬ В  
СОБЛЮДЕНИИ  
СТАНДАРТА**



**ISO/IEC 27001**

**РЕАЛИЗАЦИЯ  
БОЛЬШИНСТВА  
КОНТРОЛЕЙ  
СТАНДАРТА**



## Как использовать Стахановец легально:



В соответствии со **ст.15 Трудового кодекса РФ**, работник должен подчиняться правилам внутреннего трудового распорядка. Среди основных обязанностей работника (**ст.21 Трудового кодекса РФ**) предусмотрены такие обязанности как: добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором, соблюдать трудовую дисциплину.

Согласно **ст. 22** работодатель имеет право требовать от работников исполнения ими трудовых обязанностей.

Согласно **ст. 91**, рабочее время - время, в течение которого работник в соответствии с правилами внутреннего трудового распорядка и условиями трудового договора должен исполнять трудовые обязанности.

Кроме того, условие о возможности использования работодателем программы **Стах@новец** можно включить и в трудовой договор. Данное условие можно включить в раздел "права и обязанности сторон", либо в раздел "Особые условия". Также можно использовать другой подход - руководитель предприятия издает приказ об установке ПО, с которым сотрудники должны ознакомиться и согласиться.

## Пример внедрения:

**Заказчик:** Центр энергетики, сфера деятельности – проектирование.

**Проблема:** массовые увольнения сотрудников и утечка конфиденциальной информации.



**Что показал мониторинг:** выявлены сотрудники «сливающие» информацию внутри компании, выявлены причины массового оттока сотрудников в конкурирующие организации – «слив» коммерческих тайн за вознаграждение и новую работу.

**Результат:** прекращение утечек информации и окупаемость программы за две недели.

Спасибо за внимание!



Администрация МО  
Анапа



ГАЗИНФОРМСЕРВИС



ВАНКОРНЕФТЬ



РОСНЕФТЬ



A.v.e  
сеть аптек



Администрация  
города Сургут



УДОБНЫЕ  
ДЕНЬГИ



Ростелеком



грузовая  
КОМПАНИЯ



**ЗАДАЙТЕ ВАШ ВОПРОС:  
Хотите протестировать?**



**[m.apostolov@stakhanovets.ru](mailto:m.apostolov@stakhanovets.ru)**



**По тел: +7 (495) 272-03-40  
Моб. : +7 (916) 456-81-85**