Справка по комплексу СТАХАНОВЕЦ

Содержание

Содержание 2
1. Введение 5
2. Структура комплекса: 6
2.1. Простой случай (один зал и один сервер) 7
2.2. Несколько залов и один сервер 8
2.3. Сложный случай (несколько залов и несколько серверов) 9
2.4. Работа в терминальных сессиях 10
3. Установка комплекса: 11
3.1. Быстрая установка в один клик 12
3.2. Рекомендации 13
3.3. Шаг 0. Скачивание необходимых файлов 16
3.4. Шаг 1. Установка SQL-сервера: 17
3.4.1. Выбор SQL-сервера 18
3.4.2. MS SQL Server 19
3.4.3. MySQL 23
3.5. Шаг 2. Установка программы администратора 28
3.6. Шаг 3. Установка сервера комплекса 29
3.7. Шаг 4. Установка клиентской части: 34
3.7.1. Общее описание 35
3.7.2. Установка на локальный компьютер 36
3.7.3. Установка на удаленные машины: 37
3.7.3.1. Общее описание 38
3.7.3.2. Способ 1. Установка в рабочей группе или домене 39
3.7.3.3. Способ 2. Установка только для домена 40
3.7.3.4. Способ 3. Установка через Active Directory 41
3.7.3.5. Способ 4. Установка через командную строку 49
3.7.4. Установка на смартфон (Android) 50
3.8. Шаг 5. Наблюдение для начальника 55
4. Удаление комплекса: 57
4.1. Удаление (деинсталляция) комплекса 58
5. Обновление комплекса: 59
5.1. Обновление комплекса 60
6. Глобальные настройки: 61
6.1. Пользователи базы 62
6.2. Настройки комплекса: 64
6.2.1. Общее описание настроек 65
6.2.2. Серверные настройки: 66
6.2.2.1. Общие настройки 67
6.2.2.2. Отложенный мониторинг 68
6.2.2.3. Мониторинг - Снимки экранов 69
6.2.2.4. Мониторинг - Веб-камеры 70
6.2.2.5. Мониторинг - Автопрослушка 71
6.2.2.6. Мониторинг - Теневое копирование 72
6.2.2.7. Мониторинг - Цифровые отпечатки 73
6.2.2.8. Распознавание текста (OCR) 74
6.2.2.9. Генератор отчетов - Параметры 75
6.2.2.10. Генератор отчетов - Отчеты (начальникам) 76
6.2.2.11. Генератор отчетов - Отчеты (сотрудникам) 77
6.2.2.12. Генератор отчетов - Сохранение в папку 78
6.2.2.13. Генератор отчетов - Отправка по FTP 79

6.2.2.14. Генератор отчетов - Отправка на e-mail 80
6.2.2.15. Генератор отчетов - Отправка на веб-сайт 81
6.2.2.16. Генератор отчетов - Отправка в файлообменник 82
6.2.2.17. Генератор отчетов - Угрозы 83
6.2.2.18. Генератор уведомлений - Отправка на e-mail 84
6.2.2.19. Генератор уведомлений - Отправка по SMS 85
6.2.2.20. Генератор уведомлений - Интеграция с Telegram 86
6.2.2.21. Защита клиента 87
6.2.2.22. События 88
6.2.3. Клиентские настройки (компьютера): 89
6.2.3.1. Общие настройки 90
6.2.3.2. Мониторинг - Машинное время 91
6.2.3.3. Мониторинг - Веб-камеры 92
6.2.3.4. Мониторинг - Автопрослушка 93
6.2.3.5. Мониторинг - Контроль оборудования 94
6.2.3.6. Мониторинг - Чаты-звонки 95
6.2.3.7. Сетевой драйвер 96
6.2.3.8. Выборочное наблюдение 97
6.2.3.9. Локальное хранилище 98
6.2.3.10. Запреты 99
6.2.3.11. События 100
6.2.4. Клиентские настройки (пользователя): 101
6.2.4.1. Общие настройки 102
6.2.4.2. Мониторинг - Пользовательское время 103
6.2.4.3. Мониторинг - Программы-сайты 104
6.2.4.4. Мониторинг - Вводимый текст 105
6.2.4.5. Мониторинг - Буфер обмена 106
6.2.4.6. Мониторинг - Снимки экранов 107
6.2.4.7. Мониторинг - Снимки экранов (доп.) 108
6.2.4.8. Мониторинг - Печать на принтере 109
6.2.4.9. Мониторинг - Файловые операции 110
6.2.4.10. Мониторинг - Отправка файлов 111
6.2.4.11. Мониторинг - Почта 112
6.2.4.12. Мониторинг - Чаты-звонки 113
6.2.4.13. Мониторинг - Теневое копирование 114
6.2.4.14. Мониторинг - Черный ящик 115
6.2.4.15. Мониторинг - Геолокация 116
6.2.4.16. Мониторинг - Мобильный клиент 117
6.2.4.17. Запреты 118
6.2.4.18. Угрозы 119
6.2.4.19. DLP в документах, картинках, голосе 120
6.2.4.20. Нетипичное поведение 121
6.2.4.21. События 122
6.2.4.22. Аутсорсинг 123
6.2.5. Группы 124
6.3. Структура компании 125
6.4. Досье сотрудников 126
6.5. Синхронизация с Active Directory 127
6.6. Анализатор рисков и производительности 129
6.7. Шаблоны отчетов 131
6.8. Цифровые отпечатки 132
6.9. Тарифы 133

6.10. Списки пользователей 134
6.11. Обслуживание базы 135
6.12. SQL-консоль 136
6.13. Журнал 137
7. Прочее: 138
7.1. Удаленное наблюдение через интернет 139
7.2. Настройка https-доступа 140
7.3. Перенос сервера 141
7.4. Клиентская служба 142
8. Вопросы и ответы (FAQ): 144
8.1. Вопросы лицензирования 145
8.2. Общие вопросы 146
8.3. Технические вопросы 147

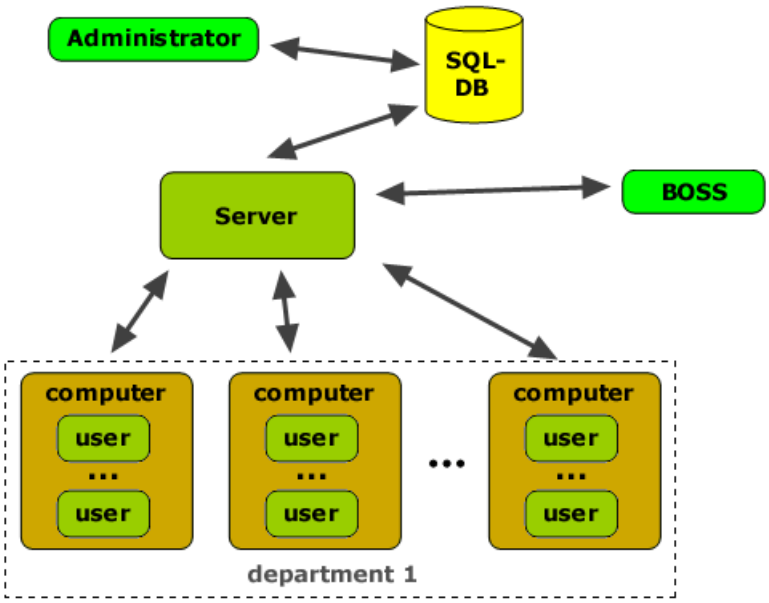
1. Введение

Комплекс **СТАХАНОВЕЦ** предназначен для наблюдения за сотрудниками на рабочих местах ПК, а также оценки эффективности их работы на основе факторов, представленных в многочисленных отчетах, формируемых программой.
ПО может использоваться в любой организации, где сотрудники работают за компьютерами.
ПО необходимо директорам и работникам отдела кадров, HR-менеджерам. Также может использоваться и для домашнего наблюдения.

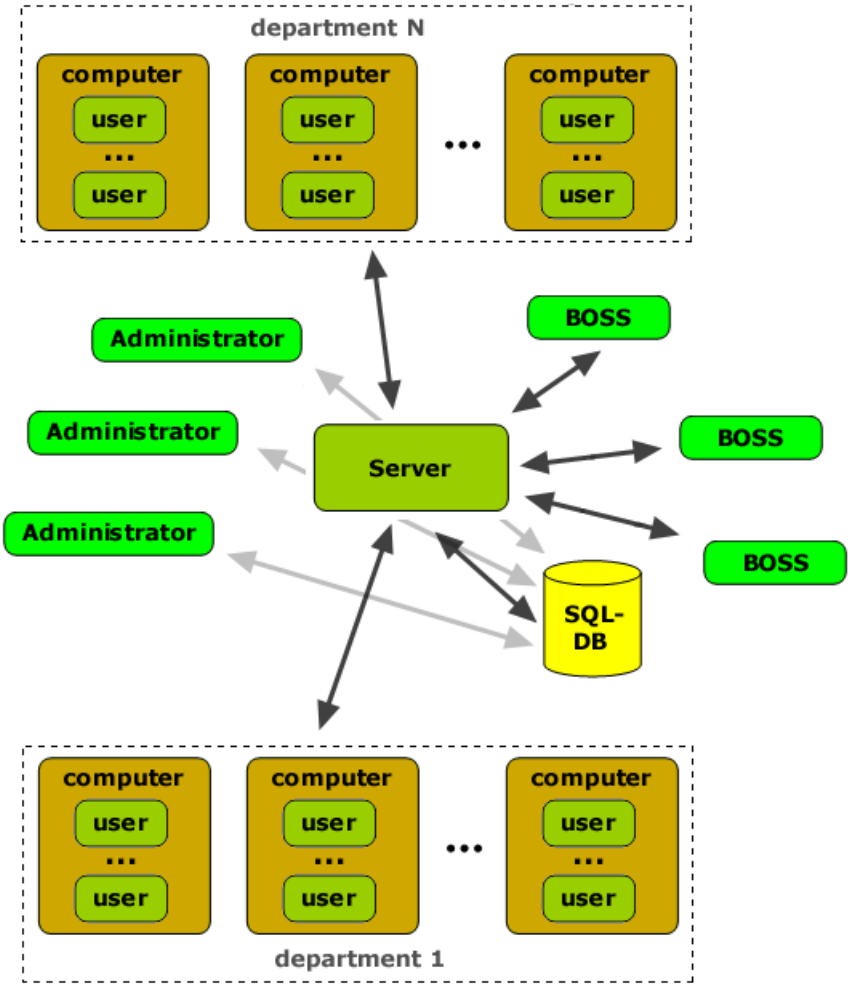
Внимание! По умолчанию в комплексе включен режим наблюдения с уведомлением, поэтому при ручной открытой установке клиента на клиентскую машину сразу будет выдано сообщение о наблюдении (еще до получения актуальных настроек комплекса от сервера), несмотря на возможность отключения в настройках комплекса этого уведомления! При удаленной установке приоритет отдается текущим настройкам комплекса.

2. Структура комплекса:

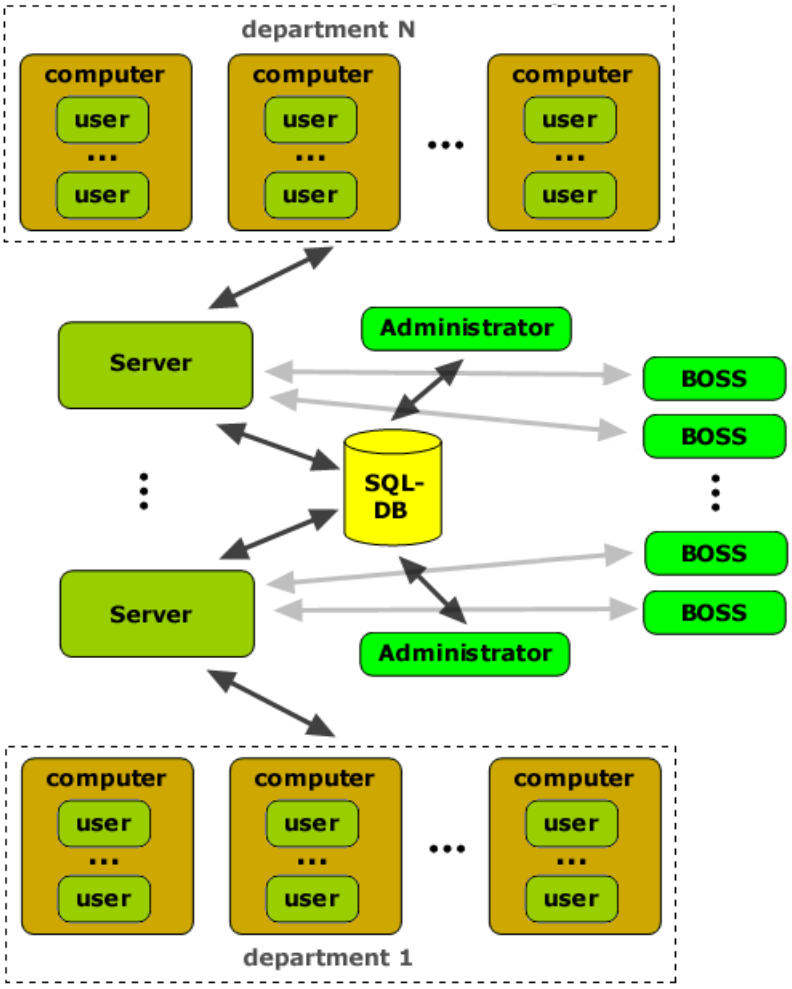
2.1. Простой случай (один зал и один сервер)



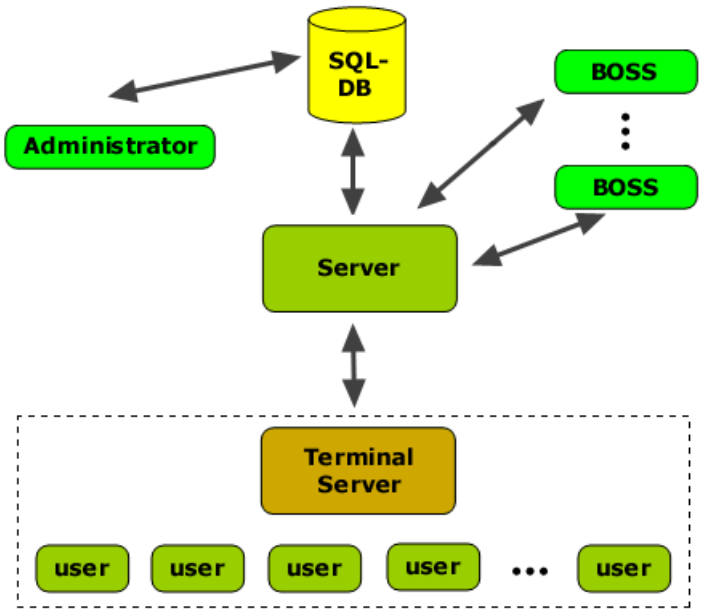
2.2. Несколько залов и один сервер



2.3. Сложный случай (несколько залов и несколько серверов)



2.4. Работа в терминальных сессиях



3. Установка комплекса:

3.1. Быстрая установка в один клик

Установка "в один клик" позволяет быстро установить серверные компоненты комплекса без каких-либо настроек. Идеально подходит для первоначального ознакомления с программой.
Для опытных системных администраторов рекомендуется использовать **полную установку (Шаг 0 - Шаг 5)**, т.к. она дает более широкие возможности.

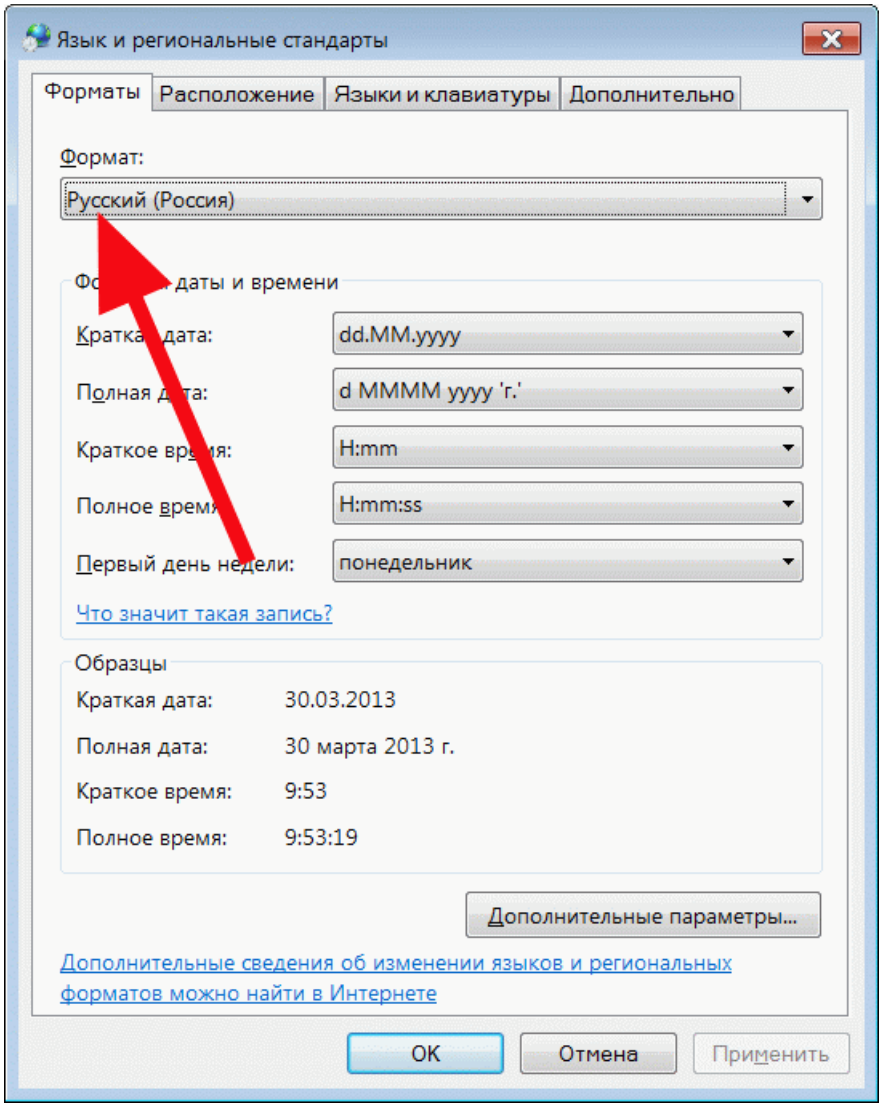
Особенности установки "в один клик":
- все серверные компоненты устанавливаются на один компьютер;
- автоматически устанавливается новая отдельная инстанция SQL Server Express;
- текущий пользователь Windows автоматически станет администратором созданной базы данных;
- SQL Express-версия имеет ограничения в 10 ГБ на базу, исп. макс. 1 ГБ ОЗУ и один CPU;
- SQL Express-версия не установится на Windows XP / Server 2003 (используйте полную установку);
- для Windows Server 2008 может потребоваться установка обновления;
- если в системе не установлен .NET 3.5 SP1 или .NET 4.0, то установщик попытается скачать и установить из интернета.

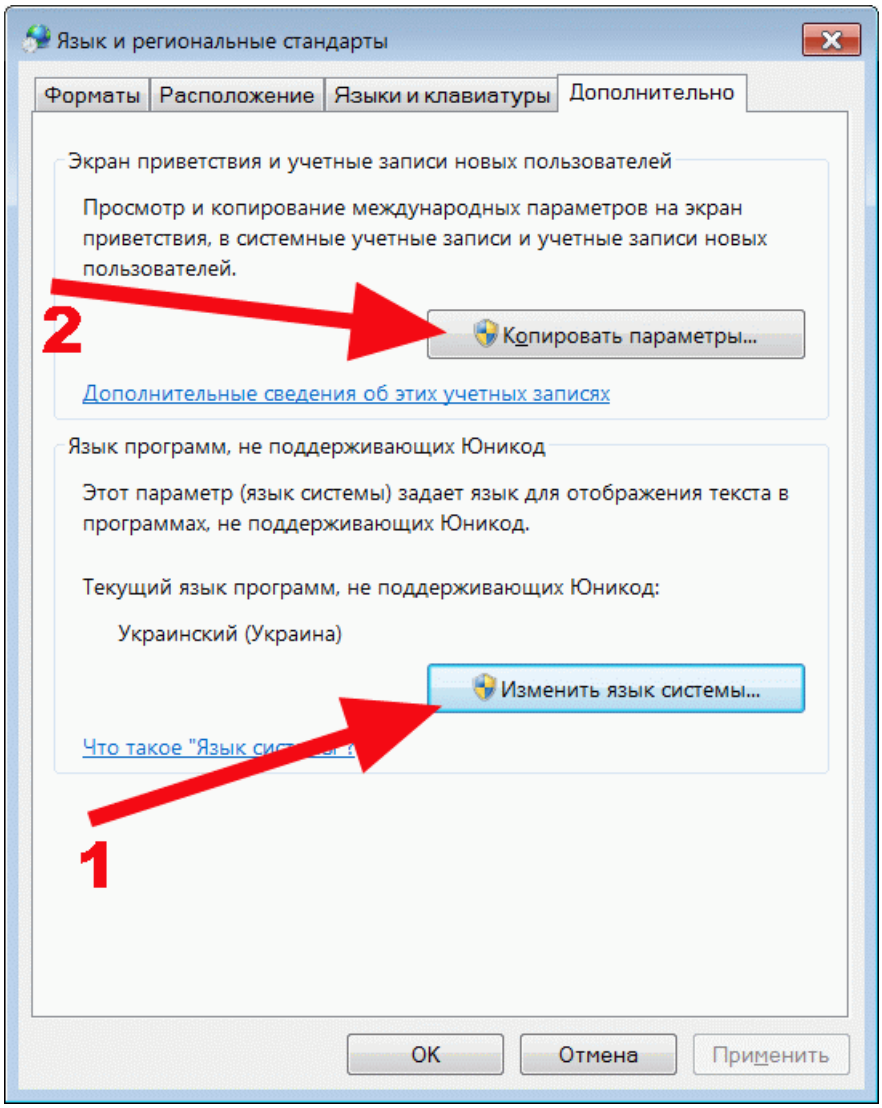
После установки можно сразу переходить к настройкам комплекса.

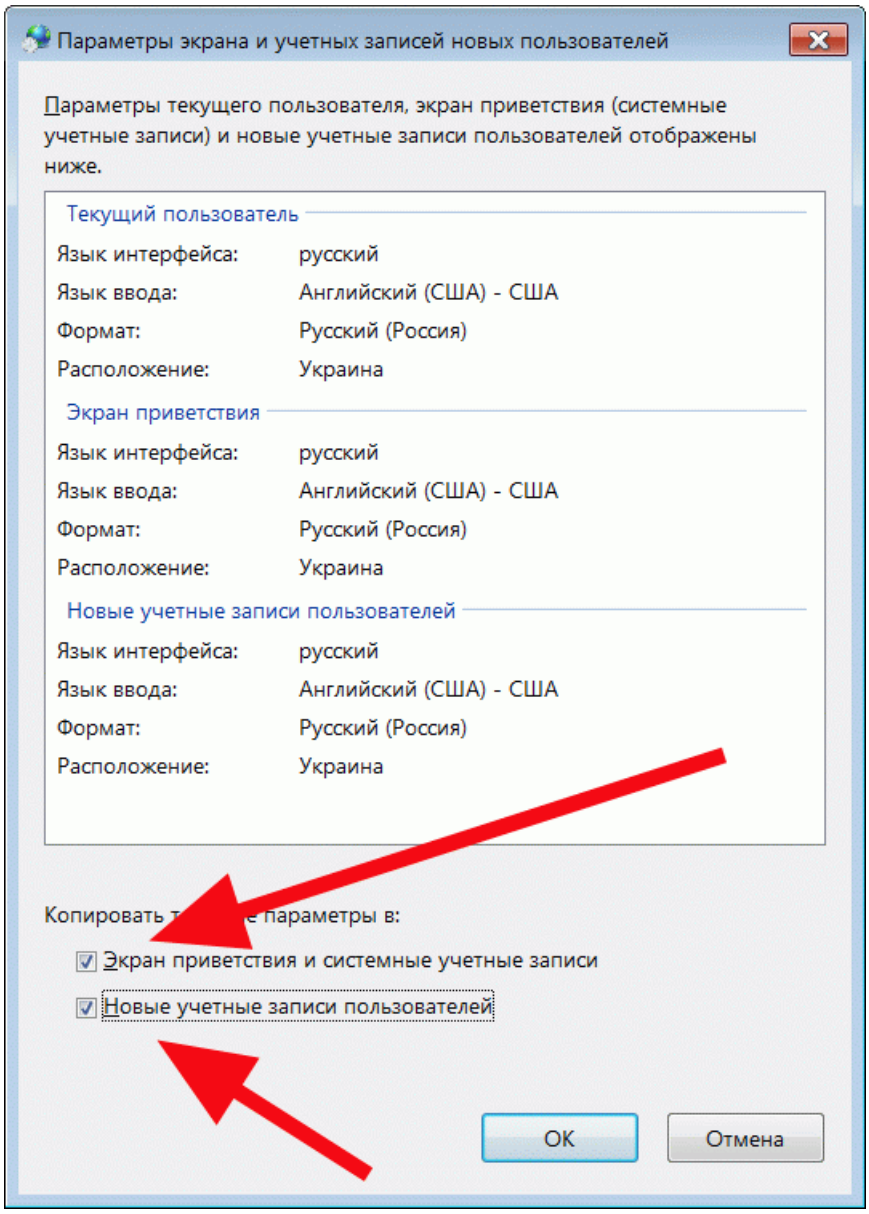
3.2. Рекомендации

Внимание! Убедитесь в том, что в языковых и региональных настройках правильно выбрано Ваше местоположение и региональные стандарты языка, а также язык по умолчанию (для не-Unicode программ) установлен на **славянский** (Русский, Украинский, Белорусский, Болгарский).
В противном случае многие надписи будут отображаться в виде знаков вопроса ("?").
Для клиентской части таких настроек **не требуется**!

Необходимо выполнить:
- установку славянского языка для не-юникод программ;
- установку славянского языка в региональных параметрах;
- распространить данные настройки на системные учетные записи;
- **перезагрузить компьютер** если вносились изменения;
- если установлен английский .NET Framework, то желательно установить русский.




Язык и региональные стандарты
Форматы
Расположение
Языки и клавиатуры
Дополнительно
Экран приветствия и учетные записи новых пользователей
Просмотр и копирование международных параметров на экран приветствия, в системные учетные записи и учетные записи новых пользователей.
2
Копировать параметры...
Дополнительные сведения об этих учетных записях
Язык программ, не поддерживающих Юникод
Этот параметр (язык системы) задает язык для отображения текста в программах, не поддерживающих Юникод.
Текущий язык программ, не поддерживающих Юникод:
Украинский (Украина)
Изменить язык системы...
1
OK
Отмена
Применить


Параметры экрана и учетных записей новых пользователей
Параметры текущего пользователя, экран приветствия (системные учетные записи) и новые учетные записи пользователей отображены ниже.
Текущий пользователь
Язык интерфейса: русский
Язык ввода: Английский (США) - США
Формат: Русский (Россия)
Расположение: Украина
Экран приветствия
Язык интерфейса: русский
Язык ввода: Английский (США) - США
Формат: Русский (Россия)
Расположение: Украина
Новые учетные записи пользователей
Язык интерфейса: русский
Язык ввода: Английский (США) - США
Формат: Русский (Россия)
Расположение: Украина
Копировать параметры в:
Экран приветствия и системные учетные записи
Новые учетные записи пользователей
OK
Отмена

3.3. Шаг 0. Скачивание необходимых файлов

Выберите SQL-сервер (необходим для работы):

Microsoft SQL Server 2014 Express
Microsoft SQL Server 2008 Express (рекомендуется только для старых ОС)
MySQL Server

Прочее (опционально):

Клиентская часть для Android
Утилита интеграции с системой СКУД
Утилита для установки на print-серверы (если есть "расшаренные" принтеры)
Утилита для печати перехваченных файлов принтера (.SPL)
Утилита для отправки SMS через USB-модем
Утилита для отправки SMS через http SMS-шлюз
Утилита для дешифрации mp4-файлов "черного ящика" (mp4decrypt)
Пример получения данных из SQL-базы комплекса через сторонний скрипт

Системные требования к ПО:

Сервер:	XP(SP3)/Vista/Win7/2008/Win8/2012/Win10/2016 и более поздние ОС (32/64-бит)
Клиент:	XP(SP3)/2003/Vista/Win7/2008/Win8/2012/Win10/2016 и более поздние ОС (32/64-бит)
Мобильный клиент:	Android 4.4.2/5.0/5.1/6.0/7.0/8.0
SQL-сервер:	MS SQL Server, MySQL
Работа в терминалах:	поддерживается

3.4. Шаг 1. Установка SQL-сервера:

3.4.1. Выбор SQL-сервера

SQL-база необходима для хранения всех клиентских настроек, отчетов пользователей, прав доступа и пр.
В данной версии ПО поддерживаются MS SQL Server и MySQL
Внимание! Синхронизация с Active Directory возможна только при использовании **MS SQL Server** (**MySQL не поддерживается!**).
Установочные файлы скачиваются на предыдущем шаге и доступны для **бесплатного** использования в соотв. с лицензией Microsoft (информация для MS SQL)

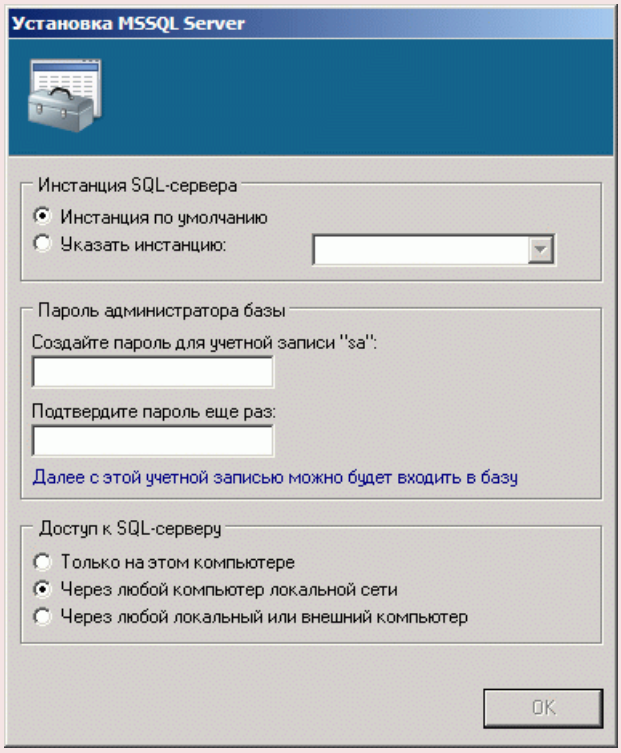
Выберите используемый сервер по желанию:

MS SQL Server
MySQL

3.4.2. MS SQL Server

Если ранее SQL-сервер не был установлен

Саму установку, как правило, необходимо производить на отдельную серверную машину, либо на машину администратора (если отдельной серверной нет).
Установка запустится только из-под учетной записи **администратора** компьютера!



Первым запрашиваемым параметром в ходе установки является **инстанция** SQL-сервера.
В большинстве случаев SQL-база устанавливается в одном экземпляре на одну машину, потому необходимо оставить "Инстанция по умолчанию". Однако, если же вы желаете установить несколько экземпляров SQL-сервера на одну машину, то необходимо вписать уникальное имя инстанции.
В этом случае каждая инстанция представляет собой независимый SQL-сервер со своей базой СТАХАНОВЕЦ, в которой будут содержаться свои настройки, отчеты, пользователи, права и пр.
В такой архитектуре необходимо также инстанцировать и сервер комплекса СТАХАНОВЕЦ, чтобы каждая инстанция сервера СТАХАНОВЕЦ подключалась к своей инстанции SQL-сервера. Клиентские машины также должны выборочно подключаться к той или иной инстанции сервера комплекса СТАХАНОВЕЦ. А администратору необходимо создать базу данных и выполнить настройки для каждой инстанции SQL-сервера. В итоге каждый начальник сможет наблюдать через БОСС-Онлайн только за своим отделом, просматривать отчеты из базы SQL только своего отдела и по возможности менять настройки (если на то администратор выдаст ему права) только для своего отдела.
В вышеописанном случае при подключении к нужной инстанции SQL-сервера необходимо указывать не только имя машины, но и имя инстанции:
machine\instance, например: **SERVER\inst1**

Далее в ходе установки нужно создать новый пароль для встроенной учетной записи администратора со спец. логином **"sa"**.
Потом с этим логином можно будет входить в базу для изменения всех настроек.
По умолчанию **текущий пользователь Windows будет также добавлен как администратор базы**.

Также предлагается выбрать область видимости SQL-сервера в зависимости от конфигурации сети и ваших потребностей.

Если уже установлен MS SQL Server

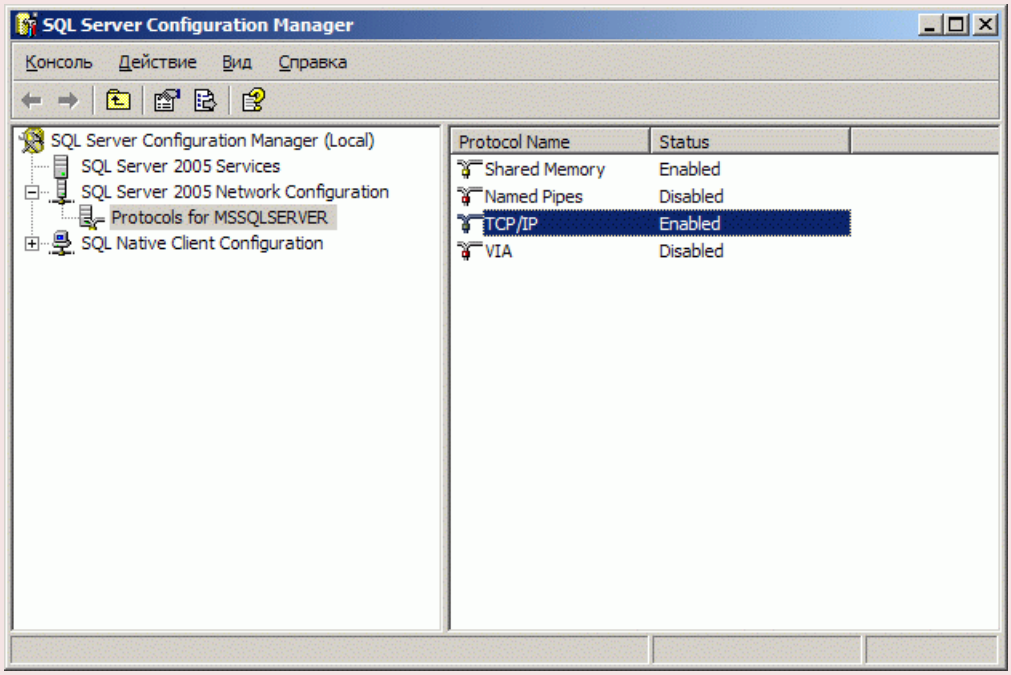
Если уже установлен MS SQL Server, то необходимо просто проверить его конфигурацию.

Внимание!!! Если ранее SQL-сервер был установлен с инстанцией отличной от инстанции по умолчанию, или установлен в нескольких инстанциях, то при подключении к серверу необходимо указывать не только имя машины или ее IP-адрес, но и имя инстанции или ее порт.
Например: SERVER\Instance1 или 192.168.1.10,1433
Имя инстанции можно посмотреть через "SQL Server Configuration Manager". Инстанция по умолчанию носит

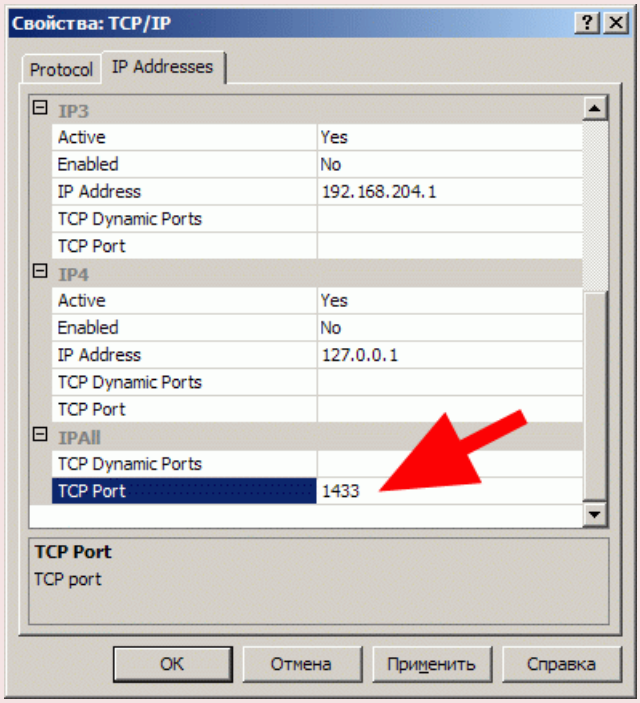
имя "MSSQLSERVER".
Для удаленного доступа к инстанции, отличной от инстанции по умолчанию, необходимо включение службы "SQL Server Browser" на сервере, что также удобно сделать через "SQL Server Configuration Manager".

Если режим аутентификации сервера установлен как **"аутентификация Windows"**, то работать комплекс не сможет! В этом случае его рекомендуется изменить на **"смешанный"**.
Это можно сделать в системном реестре:
HKLM\SOFTWARE\Microsoft\Microsoft SQL Server\MSSQL.<InstanceId>\MSSQLServer\LoginMode установить в **2** после чего перезапустить службу SQL-сервера!

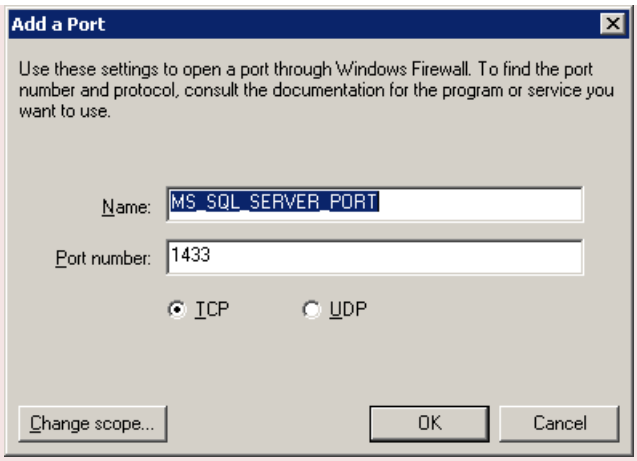
Далее нужно проверить, есть ли доступ к серверу через сеть в случае удаленного расположения SQL-сервера.
Для этого запустите утилиту сервера **SQL Server Configuration Manager** (через меню "ПУСК")
и проверьте, чтобы был включен протокол TCP/IP:



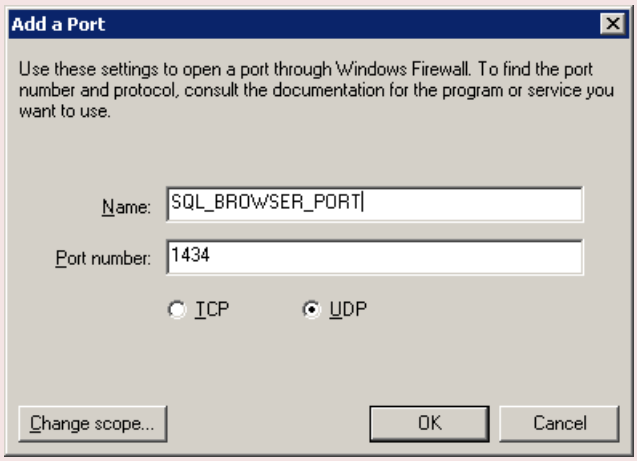
Также необходимо установить порт **1433** (или другой) в свойствах протокола:



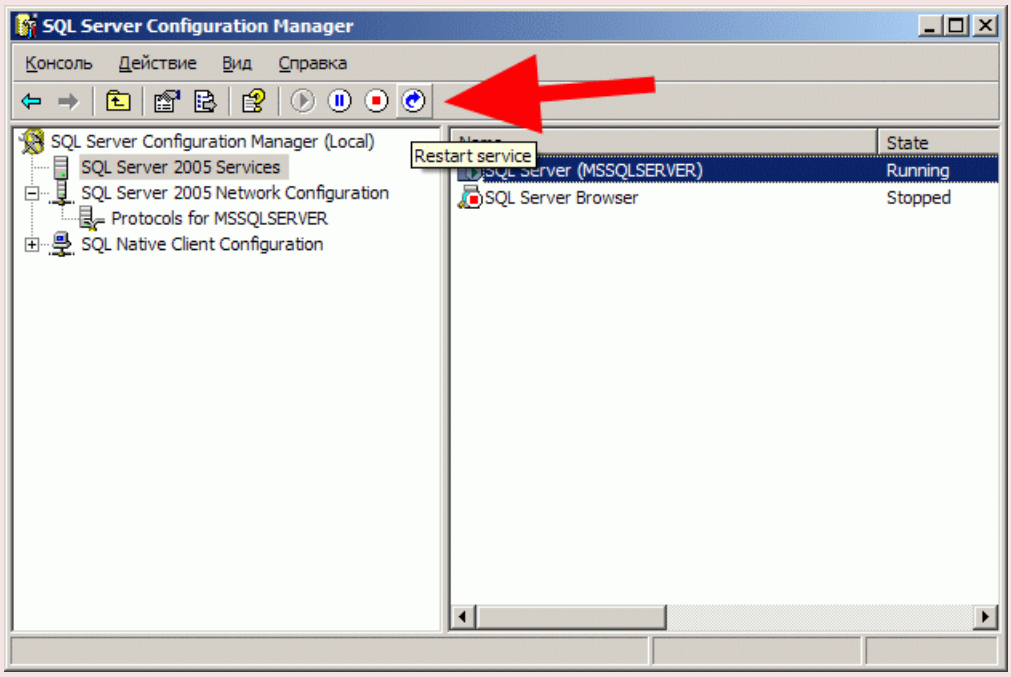
Также убедитесь, что в вашем брандмауэре (Firewall'e) добавлен для разрешения этот TCP порт **1433** (или другой):



Также убедитесь, что в вашем брандмауэре (Firewall'е) добавлен для разрешения UDP порт **1434** (если используется инстанция отличная от инстанции по умолчанию):
(в этом случае необходимо включение службы **"SQL Server Browser"**)



После чего необходимо перезапустить сервис **MSSQLSERVER**:



Для дальнейшей работы вам необходимо знать логин и пароль администратора БД (это может быть учетная запись **"sa"** или другая), или же учетная запись Windows.

Переустановка SQL-сервера

Удаление SQL-сервера необходимо производить через "Панель управления->Установка и удаление программ".
При этом после удаления сервера файл базы СТАХАНОВЕЦ **останется** на диске.
Для повторной установки сервера его необходимо **обязательно удалить!**
Находятся файлы по след. пути: "\Microsoft SQL Server\MSSQL.<InstanceId>\MSSQL\Data\stkh.*" (зависит от версии MSSQL)
После чего можно устанавливать SQL-сервер.

3.4.3. MySQL

Если ранее MySQL-сервер не был установлен

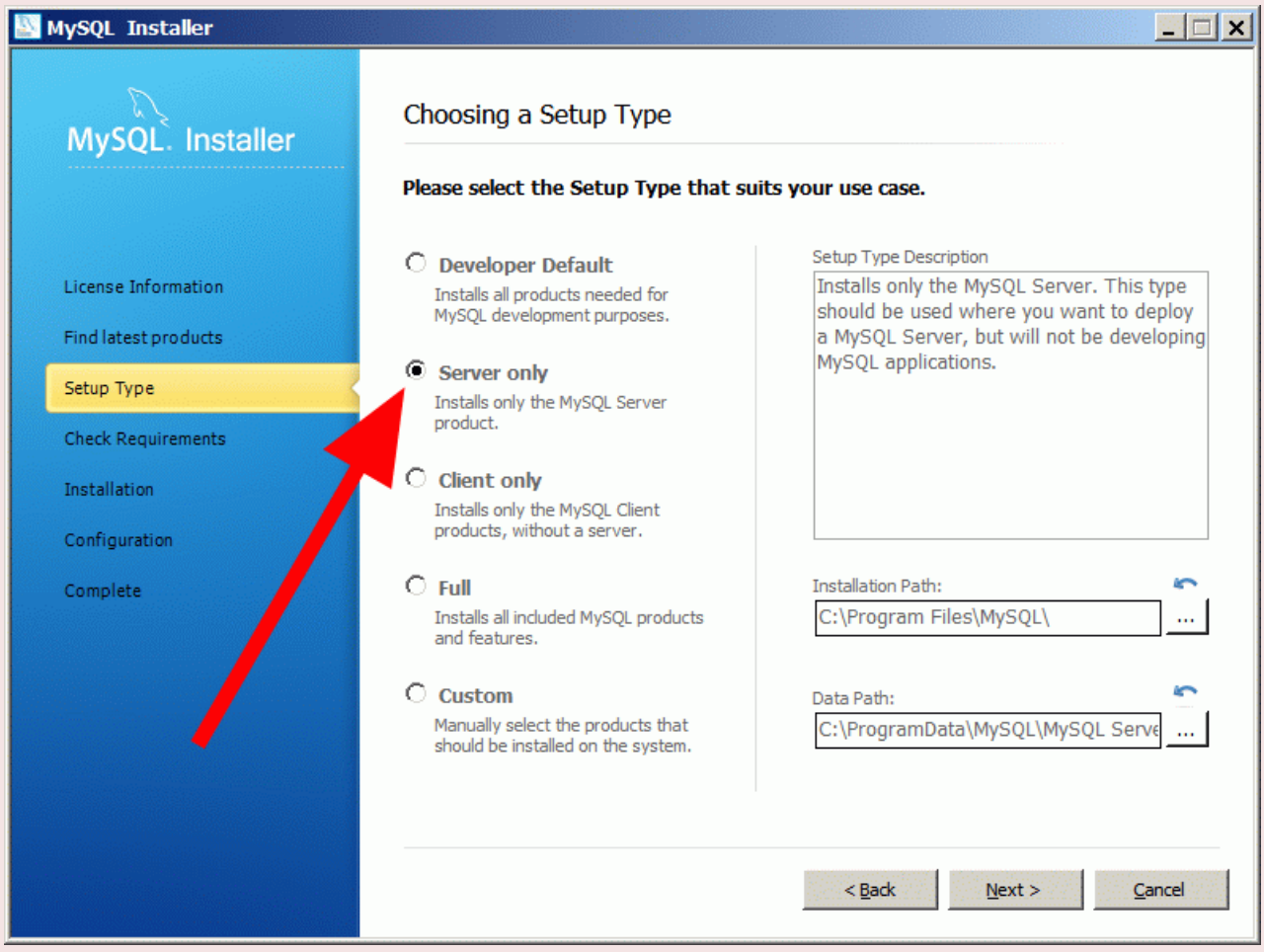
Можно устанавливать как на **Windows**, так и на **Unix**-системы.

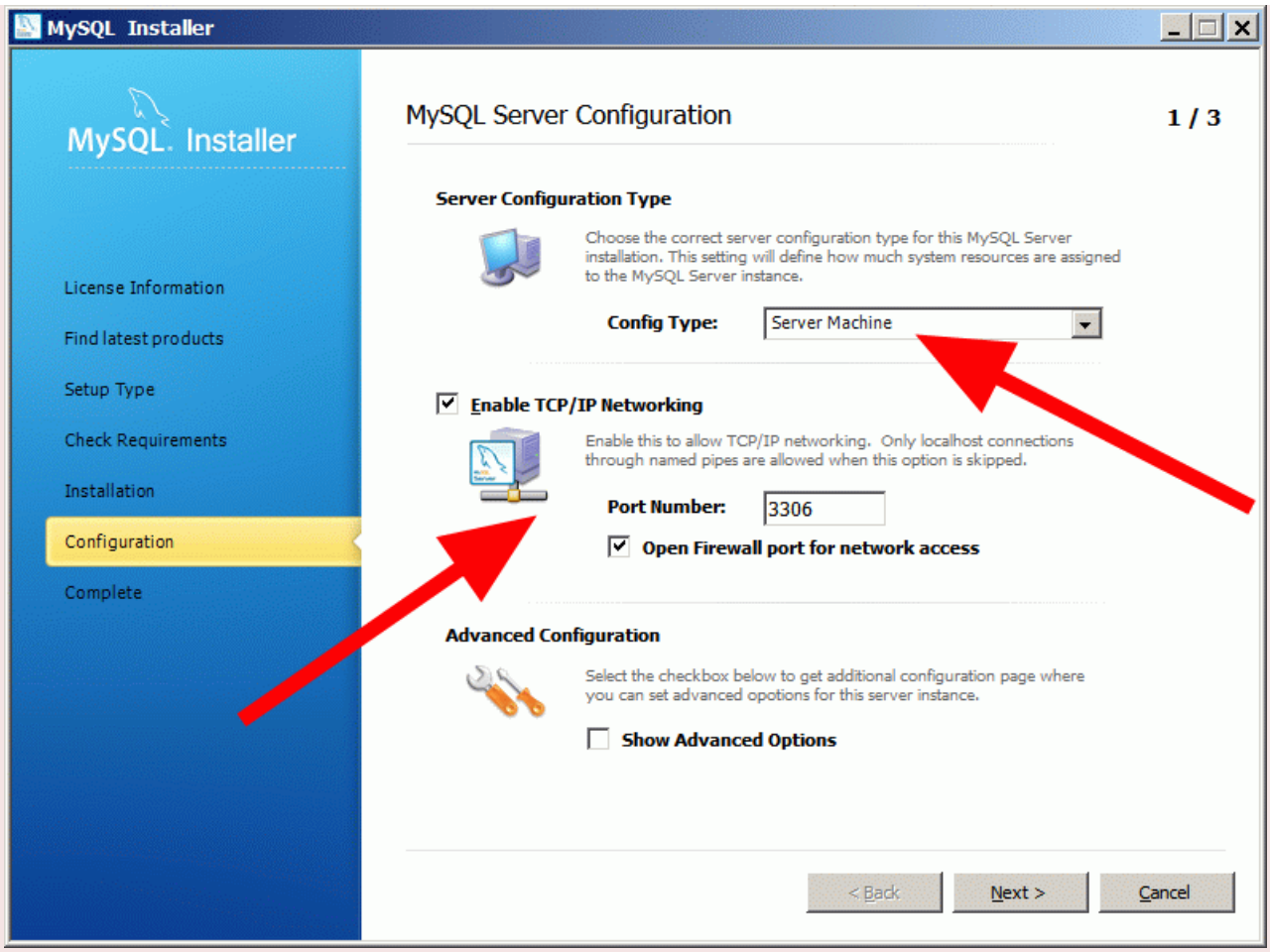
Саму установку, как правило, необходимо производить на отдельную серверную машину, либо на машину администратора (если отдельной серверной нет).

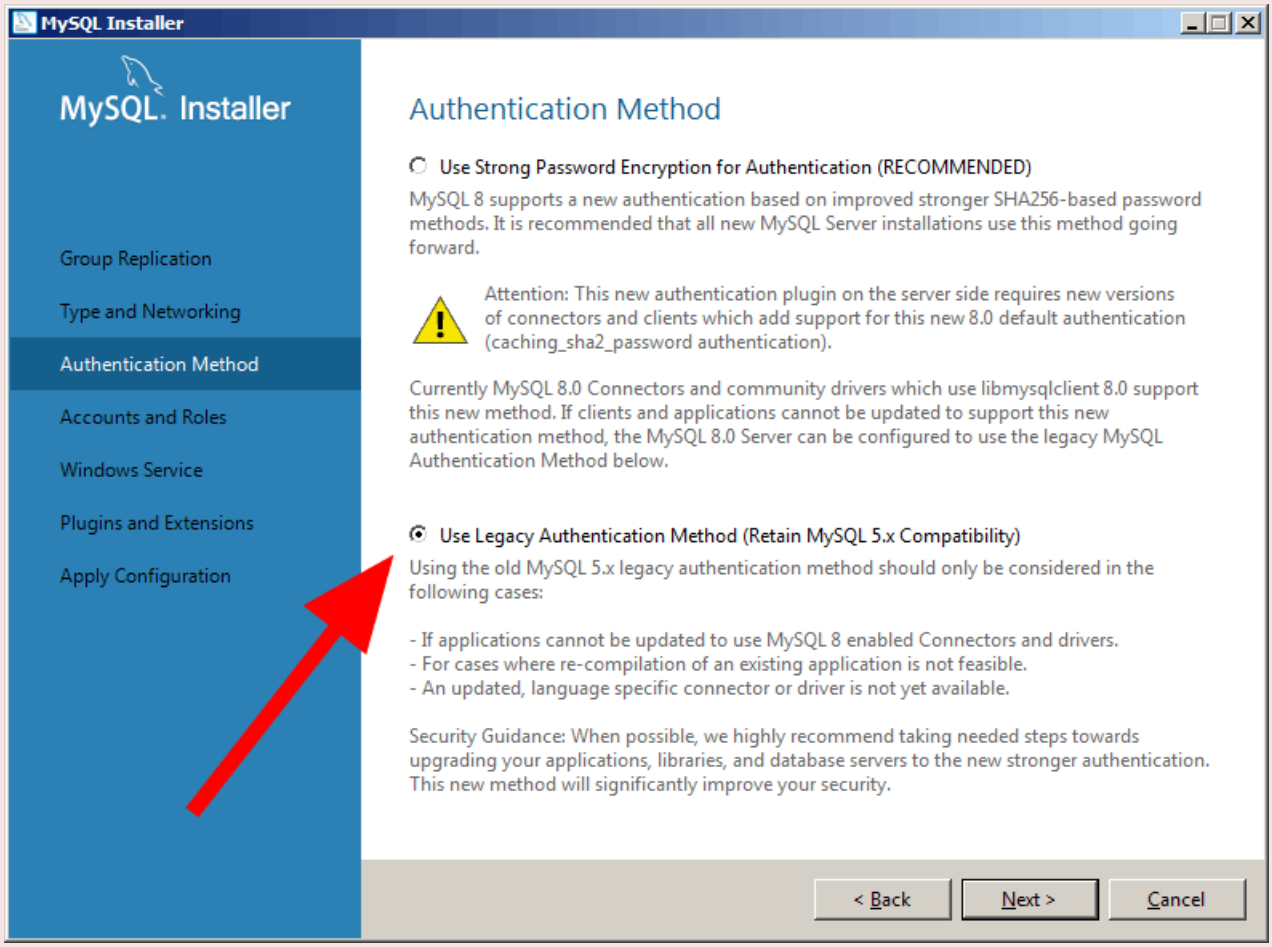
В ходе установки необходимо разрешить доступ к серверу по сети и добавить в исключения Firewall'а порт сервера (данной опции может и не быть).
В СТАХАНОВЕЦ поддерживается не только **порт 3306**, для указания другого порта нужно его указывать через двоеточие после имени сервера с MySQL при подключении (например, **SERVER:3310**).

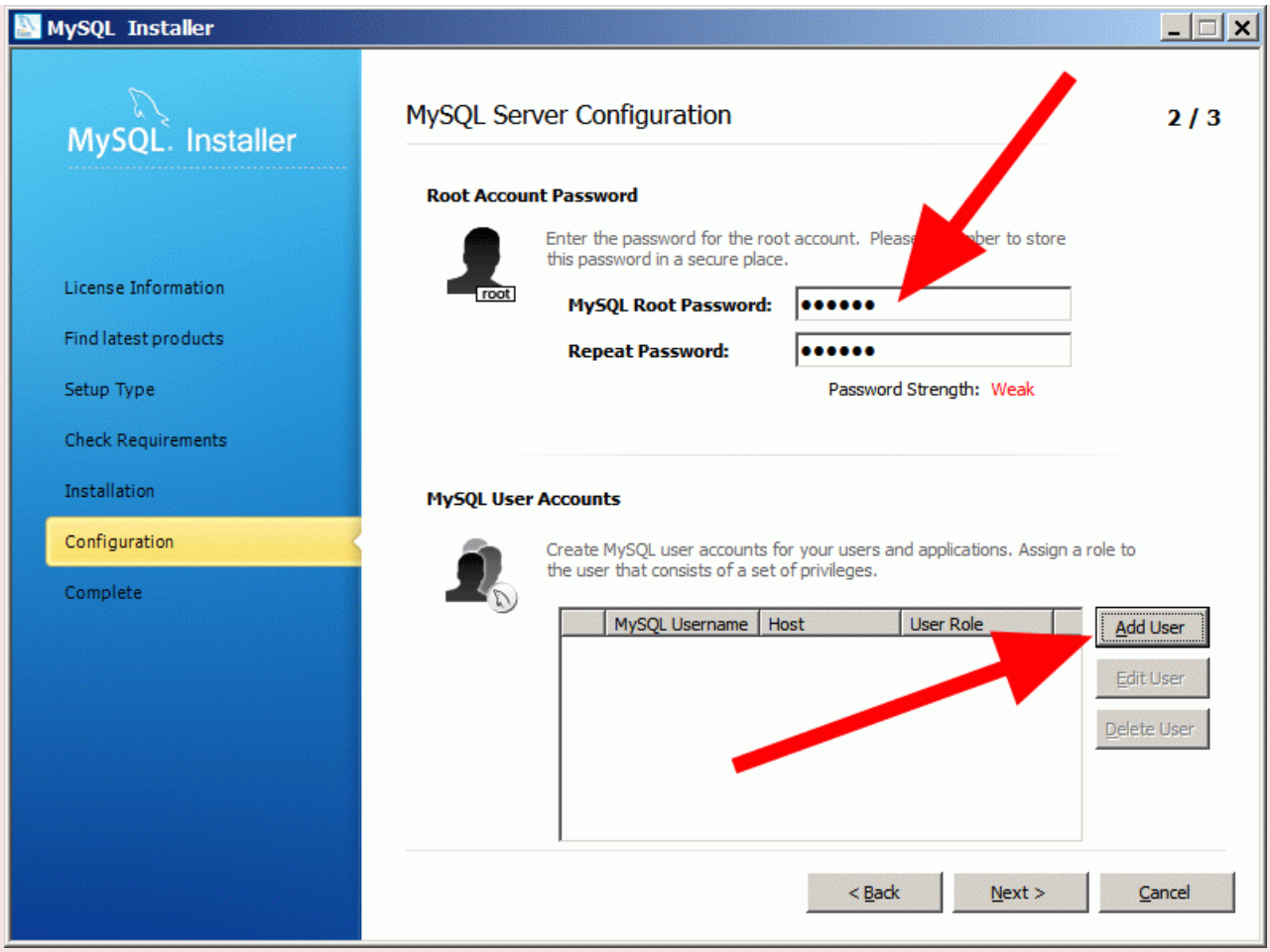
Если вам необходимо использовать несколько инстанций SQL-сервера, то в ходе установки нужно указать другое имя инстанции (сервиса для Windows), а также другой порт (отличный от порта по умолчанию 3306).

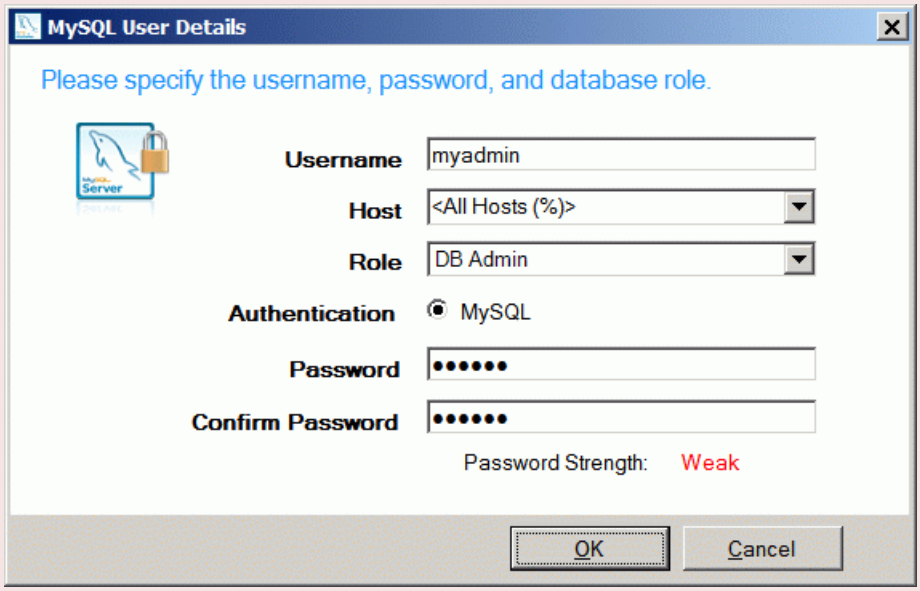
Также необходимо создать пароль для специального встроенного пользователя **"root"**. Далее под этим пользователем можно будет входить в базу и изменять все настройки. Если предлагается ввести **текущий пароль** для **root**, то оставьте это поле **пустым**!
Нужно не забыть этому пользователю разрешить доступ к базе с удаленных машин, отметив соотв. опцию в настройках (ее может не быть).
Внимание! Если база MySQL будет расположена на отдельной машине или на локальной, но при подключении используется имя машины вместо **localhost**, то по умолчанию под пользователем **root** подключиться будет нельзя! Для этого рекомендуется создать дополнительного пользователя с правами **"DB Admin"** (см. ниже), и все администраторские действия с базой осуществлять от его имени, а не от **root**!

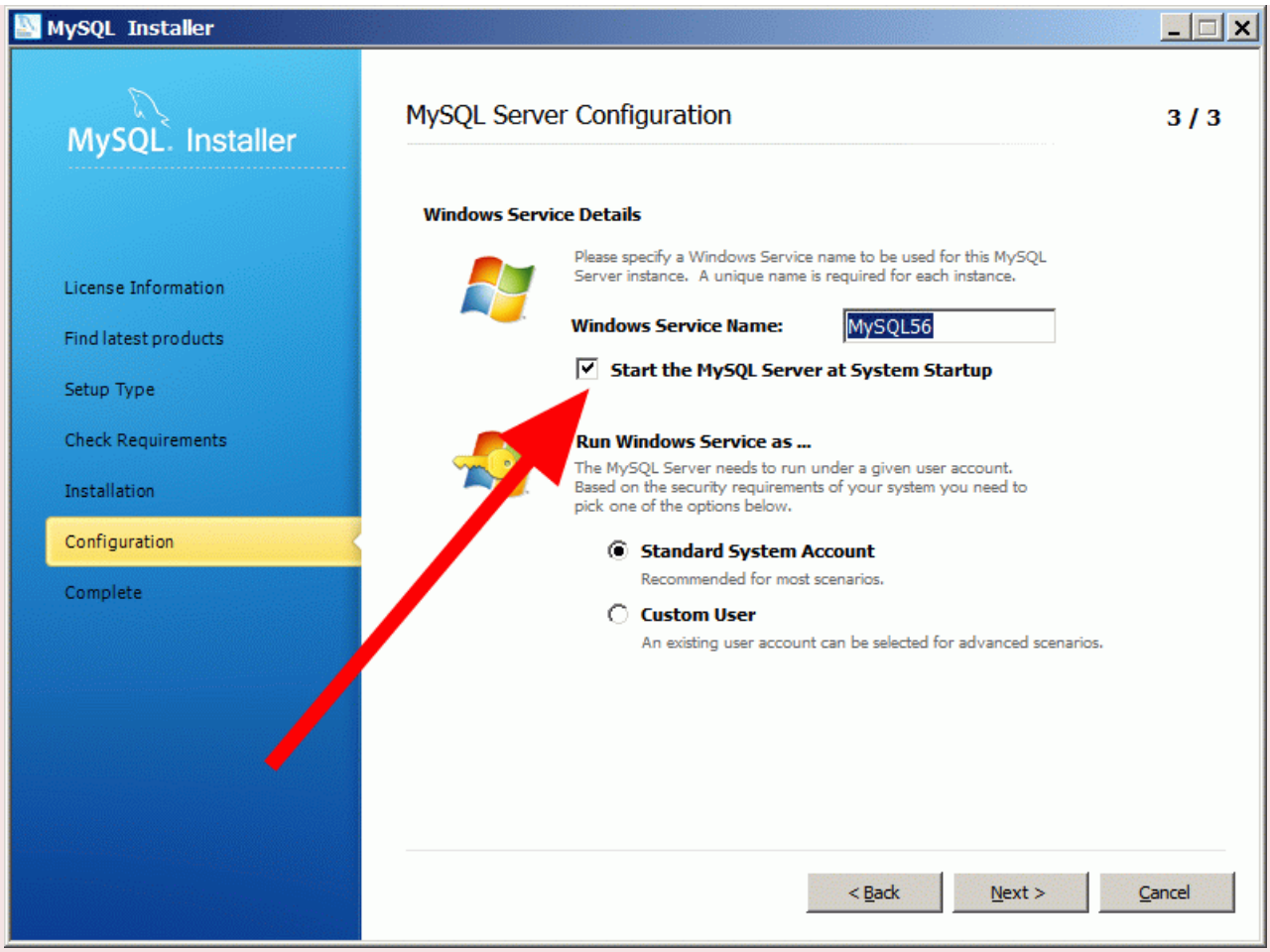



MySQL Installer
MySQL. Installer
License Information
Find latest products
Setup Type
Check Requirements
Installation
Configuration
Complete
MySQL Server Configuration
1 / 3
Server Configuration Type
Choose the correct server configuration type for this MySQL Server installation. This setting will define how much system resources are assigned to the MySQL Server instance.
Config Type:
Server Machine
Enable TCP/IP Networking
Enable this to allow TCP/IP networking. Only localhost connections through named pipes are allowed when this option is skipped.
Port Number:
3306
Open Firewall port for network access
Advanced Configuration
Select the checkbox below to get additional configuration page where you can set advanced opotions for this server instance.
Show Advanced Options
< Back
Next >
Cancel

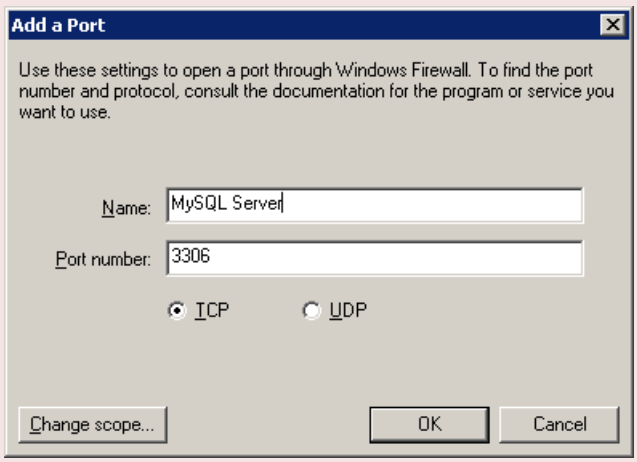

MySQL Installer
MySQL. Installer
Group Replication
Type and Networking
Authentication Method
Accounts and Roles
Windows Service
Plugins and Extensions
Apply Configuration
Authentication Method
Use Strong Password Encryption for Authentication (RECOMMENDED)
MySQL 8 supports a new authentication based on improved stronger SHA256-based password methods. It is recommended that all new MySQL Server installations use this method going forward.
Attention: This new authentication plugin on the server side requires new versions of connectors and clients which add support for this new 8.0 default authentication (caching_sha2_password authentication).
Currently MySQL 8.0 Connectors and community drivers which use libmysqlclient 8.0 support this new method. If clients and applications cannot be updated to support this new authentication method, the MySQL 8.0 Server can be configured to use the legacy MySQL Authentication Method below.
Use Legacy Authentication Method (Retain MySQL 5.x Compatibility)
Using the old MySQL 5.x legacy authentication method should only be considered in the following cases:
- If applications cannot be updated to use MySQL 8 enabled Connectors and drivers.
- For cases where re-compilation of an existing application is not feasible.
- An updated, language specific connector or driver is not yet available.
Security Guidance: When possible, we highly recommend taking needed steps towards upgrading your applications, libraries, and database servers to the new stronger authentication. This new method will significantly improve your security.
< Back
Next >
Cancel


MySQL Installer
MySQL. Installer
License Information
Find latest products
Setup Type
Check Requirements
Installation
Configuration
Complete
MySQL Server Configuration
2 / 3
Root Account Password
root
Enter the password for the root account. Please ber to store this password in a secure place.
MySQL Root Password:
Repeat Password:
Password Strength: Weak
MySQL User Accounts
Create MySQL user accounts for your users and applications. Assign a role to the user that consists of a set of privileges.
MySQL Username
Host
User Role
Add User
Edit User
Delete User
< Back
Next >
Cancel


MySQL User Details
Please specify the username, password, and database role.
Username
myadmin
Host
<All Hosts (%)>
Role
DB Admin
Authentication
MySQL
Password
Confirm Password
Password Strength: Weak
OK
Cancel



Если в установке не предлагалось добавить в исключения Firewall'а порт сервера, то необходимо это сделать вручную:



Внимание! Необходимо установить переменную сервера **max_allowed_packet** для правильной работы с комплексом СТАХАНОВЕЦ.
В файле папки MySQL-сервера **my.ini (Windows)** или **my.cnf (Unix)** в раздел **[mysqld]** необходимо добавить строчку:

max_allowed_packet=32M

После чего нужно **перезапустить** службу MySQL-сервера.

Внимание! Если данный параметр **уже прописан** в конфигурационном файле, то необходимо только изменить его значение, а не добавлять новый!

Для версии MySQL ниже 5.6 файл my.ini по умолчанию расположен в %ProgramFiles%\MySQL\MySQL Server x.xx\my.ini
Для версии MySQL от 5.6 файл my.ini по умолчанию расположен в **C:\ProgramData\MySQL\MySQL Server x.xx\my.ini**

Если уже установлен MySQL

Если уже установлен MySQL, то необходимо выполнить ряд **обязательных действий** для правильной работы СТАХАНОВЕЦ.

Для настройки установленного сервера запустите утилиту **MySQLInstanceConfig** и выполните все те же самые действия, которые описаны в предыдущем разделе:
"Если ранее MySQL-сервер не был установлен".
После чего необходимо **обязательно** настроить переменную сервера **max_allowed_packet**, о чем также написано в предыдущем разделе:
"Если ранее MySQL-сервер не был установлен".

Внимание! См. раздел **"Если ранее MySQL-сервер не был установлен"**.

Переустановка MySQL-сервера

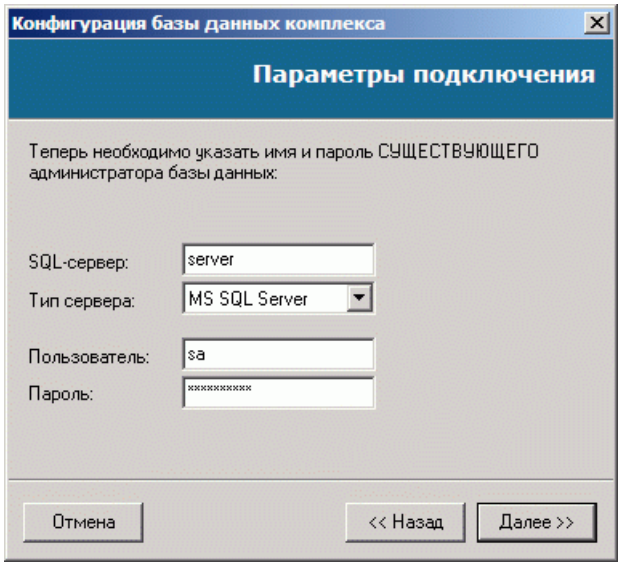
Удаление SQL-сервера необходимо производить стандартным образом через "Панель управления->Установка и удаление программ".
При этом после удаления сервера файл базы СТАХАНОВЕЦ может остаться, а может и нет (зависит от версии сервера).
Для повторной установки сервера его рекомендуется удалить (как и всю папку \MySQL), однако местоположение файлов БД также зависит от версии сервера.

3.5. Шаг 2. Установка программы администратора

Программа администратора обычно устанавливается на отдельную машину, однако при необходимости ее можно установить и на машину с SQL-сервером.
Основной задачей программы служит изменение настроек клиентских машин, настроек сервера и установка прав доп. администраторам/начальникам.
Если в вашей организации несколько администраторов на разных машинах, то можно установить данную программу сразу на несколько машин.

Установка запустится только из-под учетной записи **администратора** компьютера!

После установки запустится программа конфигурации базы данных СТАХАНОВЕЦ.
При желании эту программу всегда можно будет запустить повторно в любой момент (например, после переустановки SQL-сервера).
Данная программа создаст базу данных СТАХАНОВЕЦ на SQL-сервере и выполнит все необходимые действия для начала работы.
Программу достаточно запустить только один раз.
Для входа необходимо знать логин и пароль администратора БД. Например, пользователь **"sa"** для **MSSQL** или **"root"**, **"myadmin"** для **MySQL** (создание **"myadmin"** было описано на шаге 1).
Для **MSSQL** возможен также вход с **учетными записями Windows**:
- не указывайте пользователя и пароль для входа с **текущей учетной записью**;
- укажите пользователя в формате **DOMAIN\username** (домен без точки в сокращенном виде) для входа с **конкретной учетной записью**.



Если возникла **ошибка** выполнения и перед тем вы **переустанавливали** SQL-сервер, то необходимо **удалить файлы** старой базы СТАХАНОВЕЦ, которые остались после удаления SQL-сервера (информация только для MSSQL Server). Обычно они находятся по след. пути: "\Microsoft SQL Server\MSSQL\Data\stkh.*". После чего нужно будет запустить программу конфигурации БД **еще раз**.

После успешного выполнения база данных СТАХАНОВЕЦ полностью готова к работе и теперь нужно запустить программу **"Глобальных настроек"**. В программе сразу необходимо **добавить хотя бы одного начальника** и установить для него необходимые права. См. здесь

Далее необходимо перейти к страницам настроек клиентских машин и сервера. См. здесь
Причем можно выполнить вход в программу глобальных настроек и с новым созданным логином начальника (если ему вы обеспечили соотв. права на изменение настроек)

Опционально можно создавать **досье** на каждого сотрудника (на вкладке "Досье сотрудников"), чтобы в БОСС-Онлайн и БОСС-Оффлайн видеть привычные фамилии вместо имен пользователей системы.

Опционально можно создавать **иерархическую структуру компании** для более удобного просмотра (См. здесь).

Также доступна автоматическая **синхронизация с Active Directory** на одноименной вкладке.

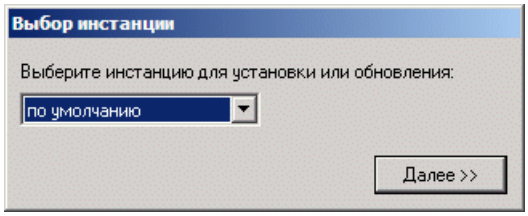
После создания начальника и установки настроек работу в программе глобальных настроек можно завершать.

3.6. Шаг 3. Установка сервера комплекса

Сервер СТАХАНОВЕЦ представляет собой системный сервис (службу) Windows, к которому подключаются все клиентские машины и программы "БОСС-Онлайн".
Сервер обычно устанавливается на отдельную машину, однако при необходимости его можно установить и на машину администратора.
На протяжении всей работы клиентских машин **сервер должен быть включен** (однако перерывы в его работе допускаются), в противном случае данные будут сохраняться на клиентских машинах до возобновления связи.
В принципе, возможна работа с несколькими серверами в одной организации, однако в большинстве случаев достаточно одного.

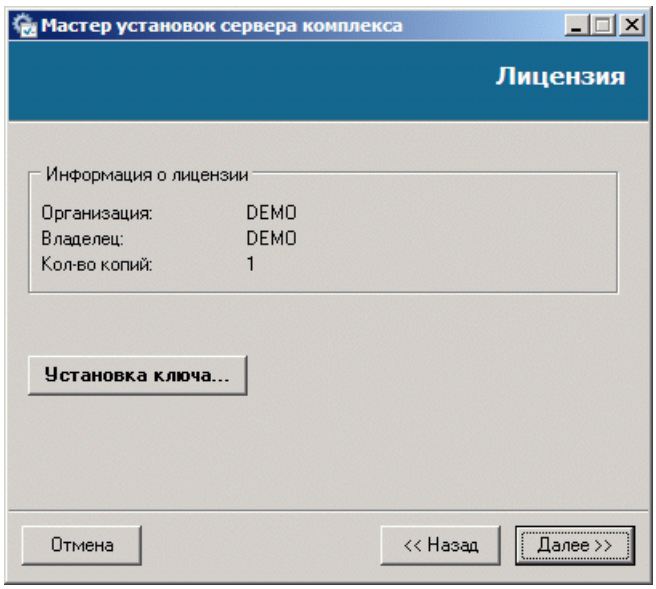
Установка запустится только из-под учетной записи **администратора** компьютера!

Сразу же будет предложено выбрать инстанцию сервера:



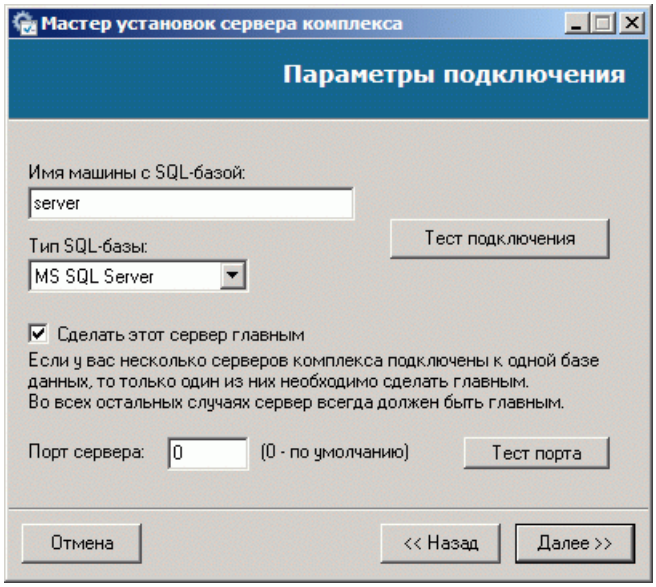
В большинстве случаев сервер комплекса устанавливается в одном экземпляре на одну серверную машину, потому необходимо оставить "по умолчанию". Однако, если же вы желаете установить несколько экземпляров сервера комплекса на одну машину, то необходимо выбрать любую уникальную инстанцию.
В этом случае каждая инстанция представляет собой независимый сервер СТАХАНОВЕЦ, к которому будут подключаться свои пользователи и который может быть подключен в свою очередь к определенной инстанции SQL-сервера.
В такой архитектуре необходимо также инстанцировать и SQL-сервер комплекса СТАХАНОВЕЦ, чтобы каждая инстанция сервера СТАХАНОВЕЦ подключалась к своей инстанции SQL-сервера. Клиентские машины также должны выборочно подключаться к той или иной инстанции сервера комплекса СТАХАНОВЕЦ. В вышеописанном случае при подключении к нужной инстанции сервера комплекса необходимо указывать не только имя машины или IP, но и порт инстанции сервера:
machine:port, например: **SERVER:12345**
О том, как выбрать порт для сервера СТАХАНОВЕЦ, будет сказано далее.

Затем запустится программа настроек сервера.
На первой ее странице предлагается активировать ключ продукта.
Внимание! Активация выполняется через интернет и привязана к оборудованию компьютера, потому активировать один и тот же ключ на разных машинах нельзя! Если у вас изменилась машина сервера, то необходимо обратиться в службу поддержки.
Кол-во копий означает кол-во одновременных клиентских подключений к серверу (учитываются подключения пользователей, не компьютеров!).



Далее необходимо указать параметры соединения с SQL-базой, а также определить главный сервер и указать порт. Если у вас несколько серверов комплекса подключены к одной SQL-базе, то только один из них необходимо сделать главным. Во всех остальных случаях сервер всегда должен быть главным!
TCP-порт сервера можно оставить 0 (по умолчанию) если вы не используете мульти-инстанций сервера. Если же у вас несколько инстанций сервера на одной машине, то для каждой из них **порт должен быть уникальным** и его нельзя оставлять "по умолчанию"!

Программу установок сервера можно запустить в любой момент для изменения настроек (при этом, если изменялся порт, то необходим перезапуск программы сервера комплекса):



В ходе установки будет установлен также и **веб-сервер Apache** в папку **%ProgramFiles(x86)%\httpd**
Веб-сервер необходим для наблюдения и просмотра отчетов через браузеры.
Веб-сервер Apache представляет собой системный сервис (службу) Windows, который "слушает" **HTTP-порт 80**
Все его настройки хранятся в файле %ProgramFiles(x86)%\httpd\conf\httpd.conf, который вы можете менять самостоятельно.
О том, как настроить доступ по **https: через SSL** см. здесь
После установки веб-сервера в Firewall Windows порт 80 будет полностью открыт. Если у вас нестандартный Firewall, то нужно добавить в его исключения либо **порт 80**, либо **%ProgramFiles(x86)%\httpd\bin\httpd.exe**
Если по каким-то причинам вы не можете использовать порт 80, то его можно изменить в %ProgramFiles(x86)%\httpd\conf\httpd.conf (изменить параметр Listen 80), после чего необходимо **перезапустить службу Apache**.

Если у вас на серверной машине **уже установлен** какой-либо веб-сервер (**Apache**, **Microsoft IIS** или другой), то программа установки обнаружит что **порт 80 занят** и установит встроенный Apache на **порт 81**.
- Если использование порта 81 в этом случае для вас приемлимо, то более ничего делать не нужно (только не забыть добавить порт при переходе на сайт: http://localhost**:81**/stkh).
- Если необходимо использовать только порт 80 и дополнительные веб-сервера не нужны, то нужно удалить дополнительные веб-сервера (например, IIS) и изменить порт встроенного Apache на 80 (см. выше как это сделать).
- Если же необходимо использовать только имеющийся у вас веб-сервер, то нужно выполнить ряд настроек самостоятельно:

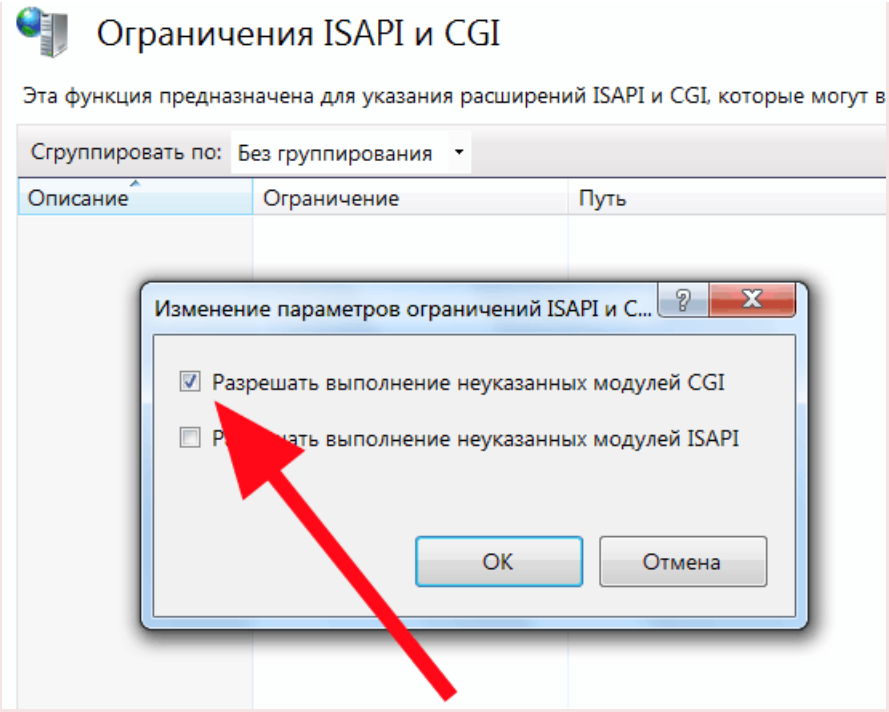
Если уже установлен веб-сервер Microsoft IIS

В этом случае необходимо просто создать виртуальный каталог на веб-сервере со ссылкой на веб-контент комплекса.
Самое главное, что нужно не забыть - **разрешить запуск CGI-программ** внутри каталога.

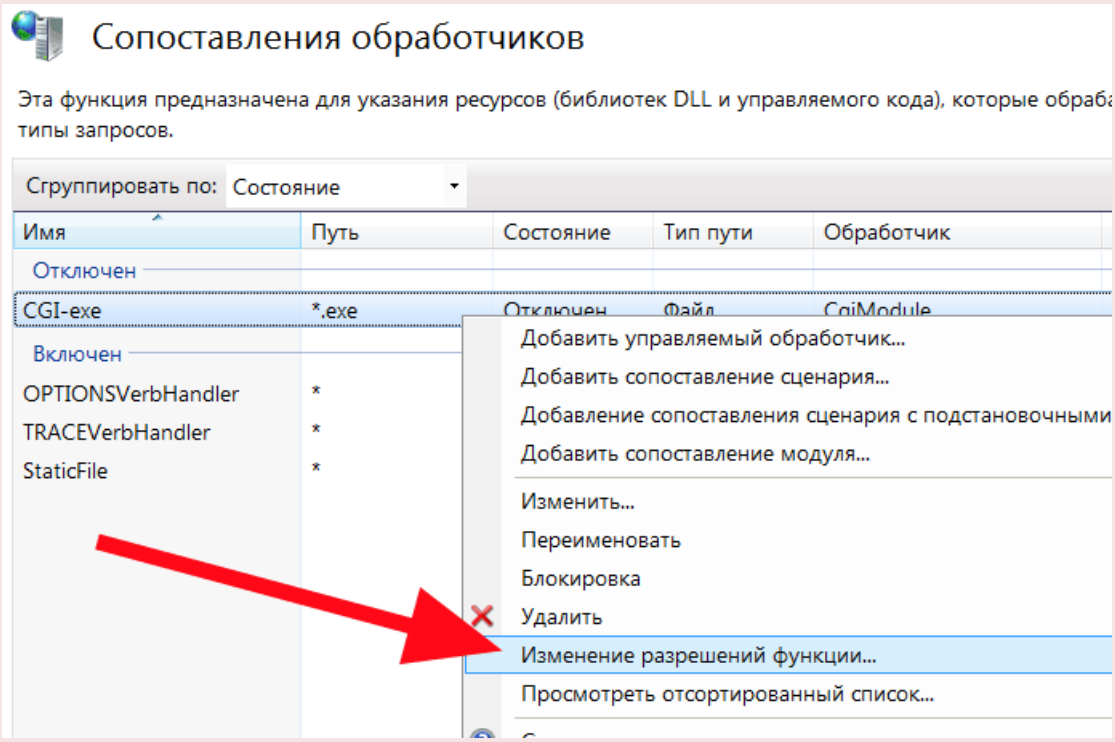
Внимание! Необходимо проверить, чтобы была **установлена поддержка CGI/ISAPI**. Если ее нет, то необходимо установить (см. **"Установка компонентов Windows"** для клиентских ОС и **"Роли сервера"** для серверных ОС).
Если установку не выполнить, то запуск CGI будет невозможен!

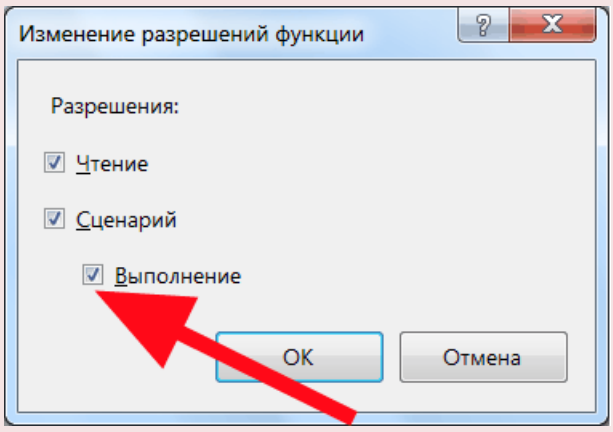
Внимание! IIS запускает CGI-скрипты комплекса в контексте специального пользователя **IUSR**, поэтому если папки **теневого копирования, скриншотов, снимков веб-камер, автопрослушки** расположены **не на диске C:** сервера, то необходимо для всех них установить **разрешение на чтение для пользователя IUSR**!

После установки CGI запускаем **inetmgr.exe** и входим в раздел сервера **"Ограничения ISAPI и CGI"** для установки разрешений:

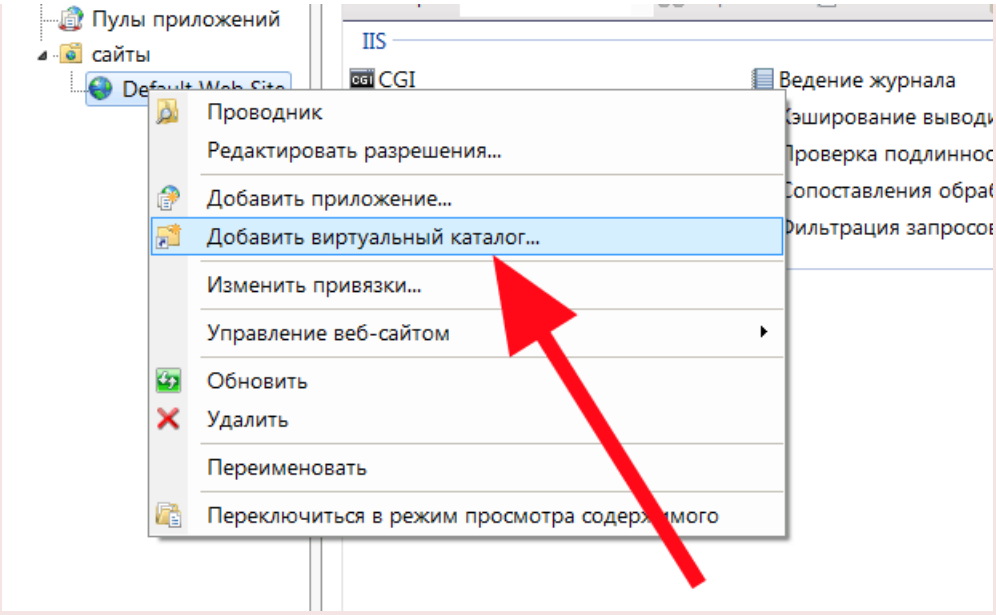


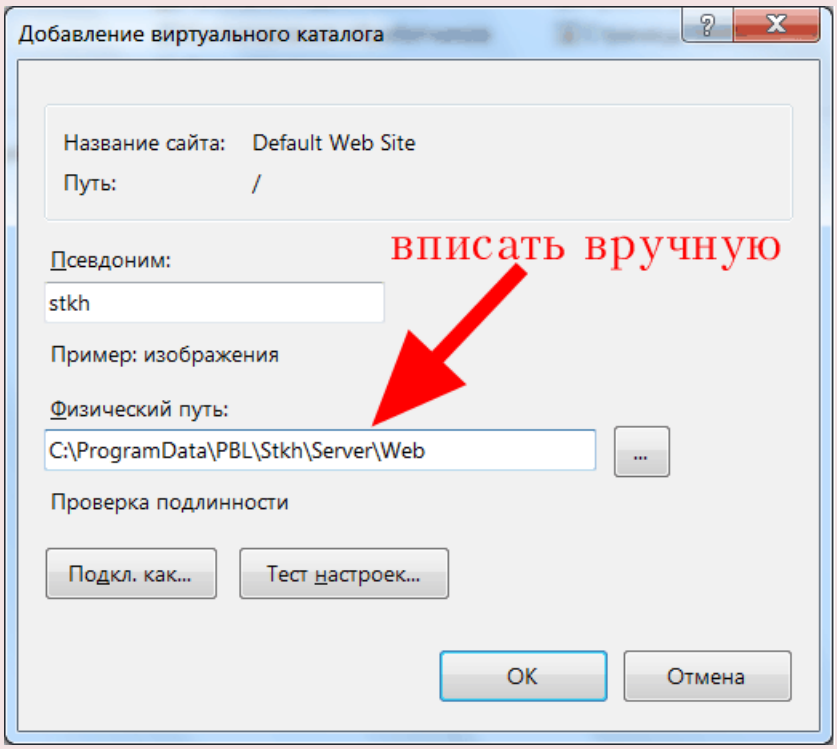
В разделе **"Сопоставление обработчиков"** сопоставляем **.exe** с **CGI-модулем**:





Далее добавляем виртуальный каталог **"stkh"** и указываем путь к папке с веб-контентом комплекса:





Если уже установлен веб-сервер Apache

В этом случае необходимо просто добавить алиас **"stkh"** со ссылкой на веб-контент комплекса.
Для **WinXP/2003** этот контент находится здесь: **"C:\Documents and Settings\All Users\Application Data\PBL\Stkh\Server\Web"**
Для **Vista/7/2008+** здесь: **"C:\ProgramData\PBL\Stkh\Server\Web"**
Самое главное, что нужно не забыть - **разрешить запуск .exe CGI-программ** внутри каталога!

Вот пример настроек (путь указан для WinXP/2003), которые нужно **добавить** в файл **httpd.conf** веб-сервера Apache:

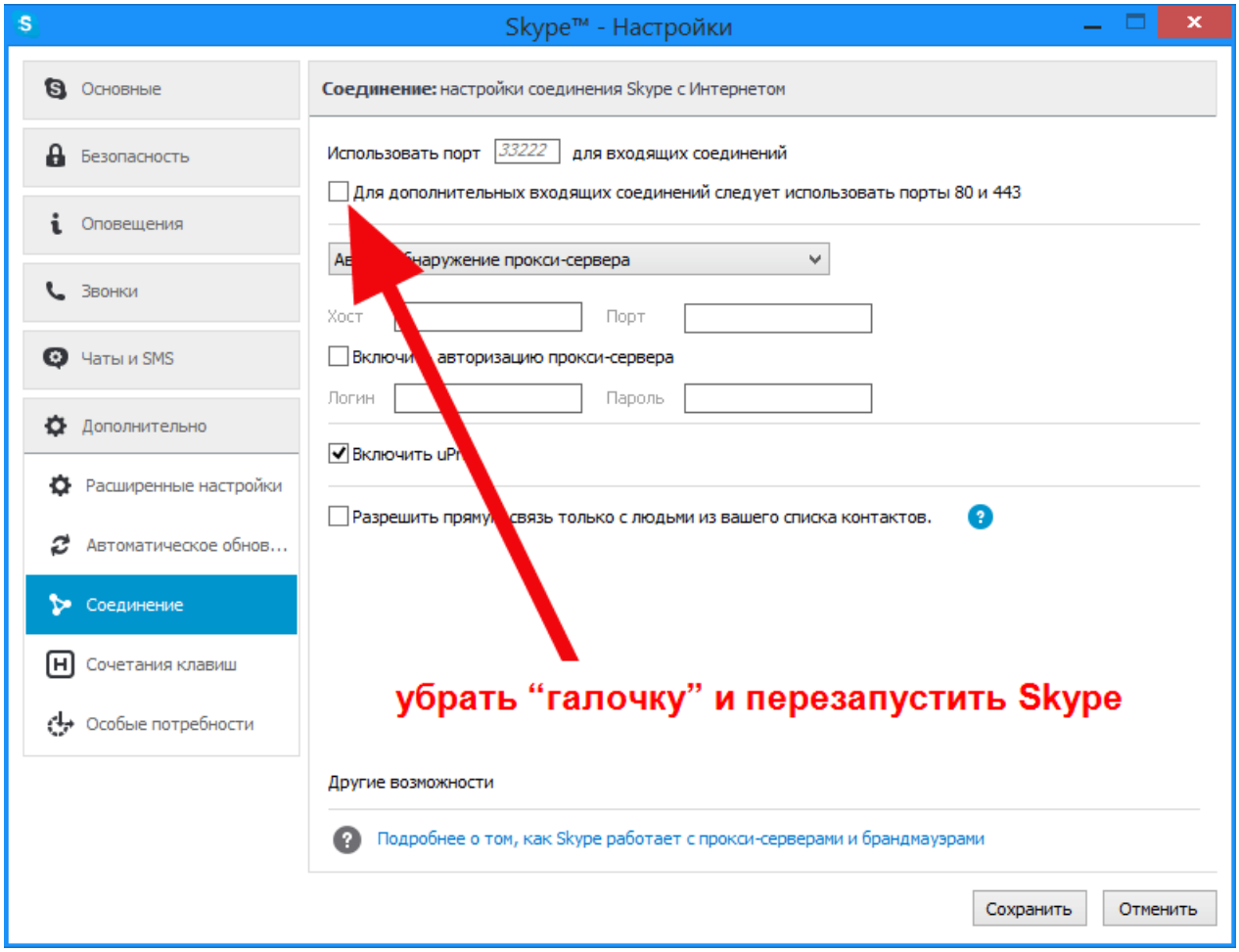
```
##############################
Alias /stkh/ "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web/"
Alias /stkh "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web/"
<Directory "C:/Documents and Settings/All Users/Application Data/PBL/Stkh/Server/Web">
    AllowOverride None
    Options FollowSymLinks ExecCGI
    Order allow,deny
    Allow from all
</Directory>
AddHandler cgi-script .exe
##############################
```

Если уже установлен другой веб-сервер

В этом случае необходимо просто добавить алиас (или виртуальный каталог) **"stkh"** со ссылкой на веб-контент комплекса.
Для **WinXP/2003** этот контент находится здесь: **"C:\Documents and Settings\All Users\Application Data\PBL\Stkh\Server\Web"**
Для **Vista/7/2008+** здесь: **"C:\ProgramData\PBL\Stkh\Server\Web"**
Самое главное, что нужно не забыть - **разрешить запуск .exe CGI-программ** внутри каталога!

Если никакой веб-сервер ранее установлен **не был**, или вы **не знаете** что такое веб-сервер, то ничего дополнительно делать **не нужно**!

Внимание! Особое внимание следует обратить на программу **Skype.** Если на этой машине запущен **Skype** и не установлено других веб-серверов, то при установке скорее всего будет выдан запрос о том, что порт 80 занят (см. выше).
Необходимо отменить следующую настройку:
Инструменты->Настройки->Дополнительно->Соединение:



После установок сервер полностью готов к работе и запущен.

Примечание: сервер использует TCP-порт **13289** по умолчанию, веб-сервер использует стандартный **HTTP-порт 80** по умолчанию.

3.7. Шаг 4. Установка клиентской части:

3.7.1. Общее описание

Клиентская часть выполняет наблюдение за пользователями и передает данные на серверную машину (если в текущий момент есть связь с сервером). Сервер записывает все данные в SQL-базу.
Клиентскую часть необходимо установить на каждую клиентскую машину только **один раз**.
В случае использования **терминального сервера** достаточно установить только лишь на терминальный сервер.

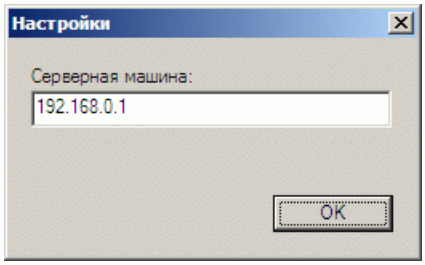
На этапе установки предлагается установить клиентскую часть на **локальный компьютер** или же выполнить установку на **удаленные машины**.
Рассмотрим оба способа подробнее.

Внимание! По умолчанию в комплексе включен режим наблюдения с уведомлением, поэтому при ручной открытой установке клиента на клиентскую машину сразу будет выдано сообщение о наблюдении (еще до получения актуальных настроек комплекса от сервера), несмотря на возможность отключения в настройках комплекса этого уведомления! При удаленной установке приоритет отдается текущим настройкам комплекса.

3.7.2. Установка на локальный компьютер

Установка запустится только из-под учетной записи **администратора** компьютера!
При этом если на компьютере предусмотрена работа нескольких пользователей, то все равно установку нужно производить только **один раз** из-под учетной записи администратора!

После установки будет автоматически запущена программа настроек:



"Серверная машина СТАХАНОВЕЦ" - необходимо установить IP-адрес сервера СТАХАНОВЕЦ (можно и имя машины). В случае подключения к нестандартному порту (или подключения к определенной инстанции сервера СТАХАНОВЕЦ) необходимо указать также и порт через двоеточие (например, **SERVER:12345**).

На этом установка клиентской части завершена.

Удалить клиентскую часть можно только через программу "БОСС-Онлайн".
Изменить настройки можно с клиентской машины (повторно запустив программу установки), либо через программу "БОСС-Онлайн".

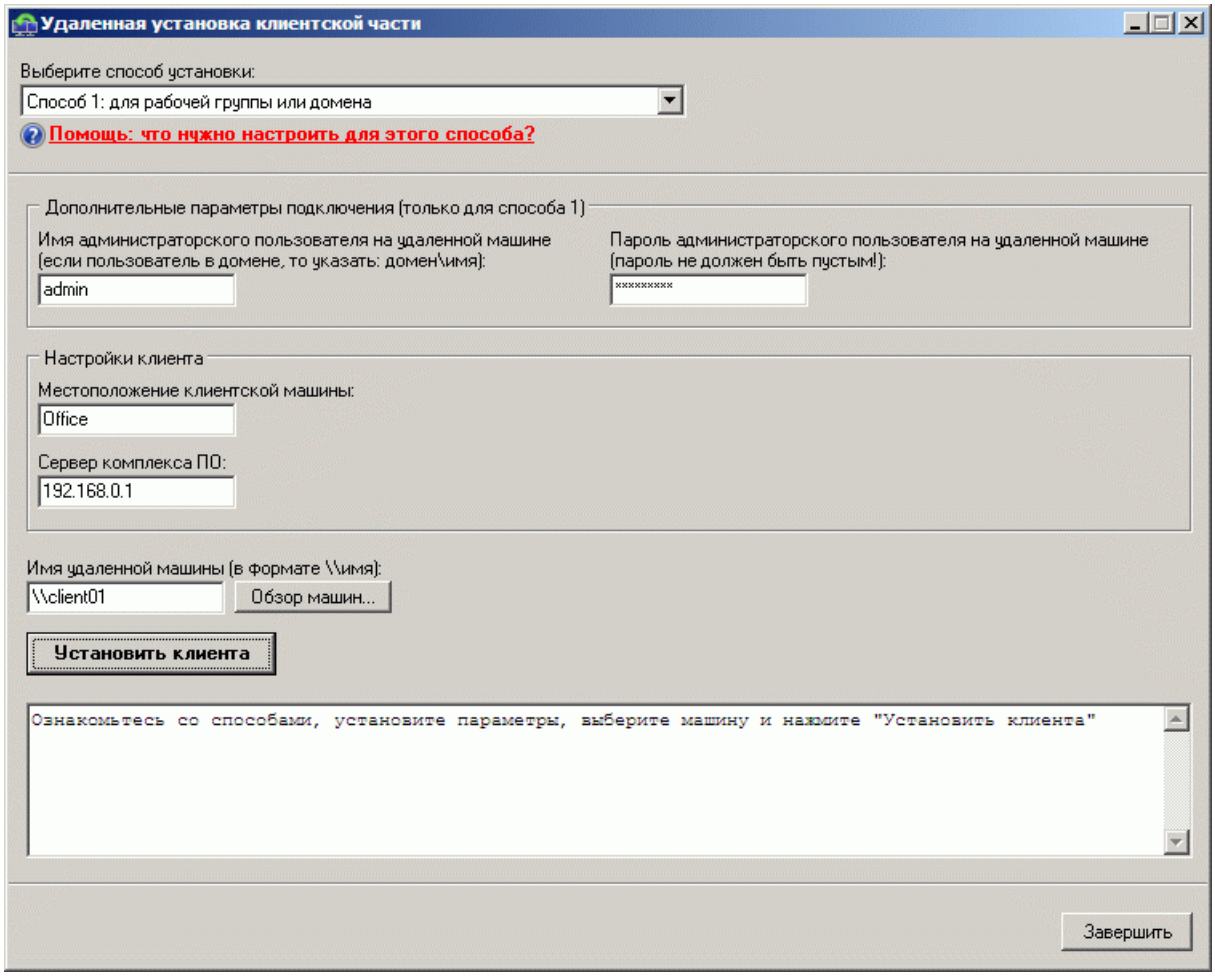
3.7.3. Установка на удаленные машины:

3.7.3.1. Общее описание

Вы можете установить клиента на удаленные машины рабочей группы или домена. При этом предусмотрено четыре различных способа в программе установки, выберите наиболее подходящий для вас.
Для удаленной установки, возможно, потребуется сделать ряд предварительных действий (особенно актуально для рабочей группы), информацию о которых см. далее по каждому способу установки.

См. также **"Автоматическое развертывание в среде Active Directory"**

Программа удаленной установки имеет следующий вид (см. ниже).
При этом настройки клиента полностью совпадают с настройками при локальной установке.



Удалить клиентскую часть можно только через программу "БОСС-Онлайн".
Изменить настройки можно повторно запустив программу установки, либо через программу "БОСС-Онлайн".

3.7.3.2. Способ 1. Установка в рабочей группе или домене

1. Необходимо знать **имя** и **пароль** администратора удаленного компьютера. Причем, администратор может быть как локальным, так и администратором домена.
Для администратора домена нужно вводить имя в формате **домен\имя**
Для локального администратора иногда требуется вводить имя в формате **компьютер\имя**

2. Необходимо проверить, "расшарена" ли общая папка **admin$** на удаленной машине. В большинстве случаев ничего делать не нужно, но для разрешения общего доступа нужно выполнить на удаленной машине:
net share admin$

3. Для рабочей группы: необходимо проверить параметр в реестре удаленной машины:
HKLM\SYSTEM\CurrentControlSet\Control\Lsa
ForceGuest типа DWORD
Необходимо, чтобы этот параметр был равен **0**
Для домена: этот параметр настраивается в политиках безопасности ("Сетевой доступ") и по умолчанию настроен так, что действие не требуется.

4. Для рабочей группы: если на удаленной машине **Windows Vista** или **Windows 7/8**, то необходимо либо отключить там UAC (контроль учетных записей пользователей), либо добавить в реестр параметр:
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
LocalAccountTokenFilterPolicy:DWORD=**1**
Для домена: действие не требуется.

5. Для **Windows XP Home Edition** этот способ может не работать!

6. Для домена: необходимо убедиться, что администратор домена не удален из списка локальных администраторов удаленного компьютера (см. "Управление компьютером"->"Локальные пользователи и группы"->"Администраторы" на удаленной машине)

См. также **"Автоматическое развертывание в среде Active Directory"**

3.7.3.3. Способ 2. Установка только для домена

1. Необходимо выполнять установку с правами администратора домена.

2. Необходимо проверить, "расшарена" ли общая папка **admin$** на удаленной машине. В большинстве случаев ничего делать не нужно, но для разрешения общего доступа нужно выполнить на удаленной машине:
net share admin$

3. Необходимо чтобы была включена служба **"Удаленный реестр"** на удаленной машине.

4. Необходимо убедиться, что администратор домена не удален из списка локальных администраторов удаленного компьютера (см. "Управление компьютером"->"Локальные пользователи и группы"->"Администраторы" на удаленной машине)

Внимание! Некоторые антивирусы на клиенте иногда могут блокировать данный способ установки.

См. также **"Автоматическое развертывание в среде Active Directory"**

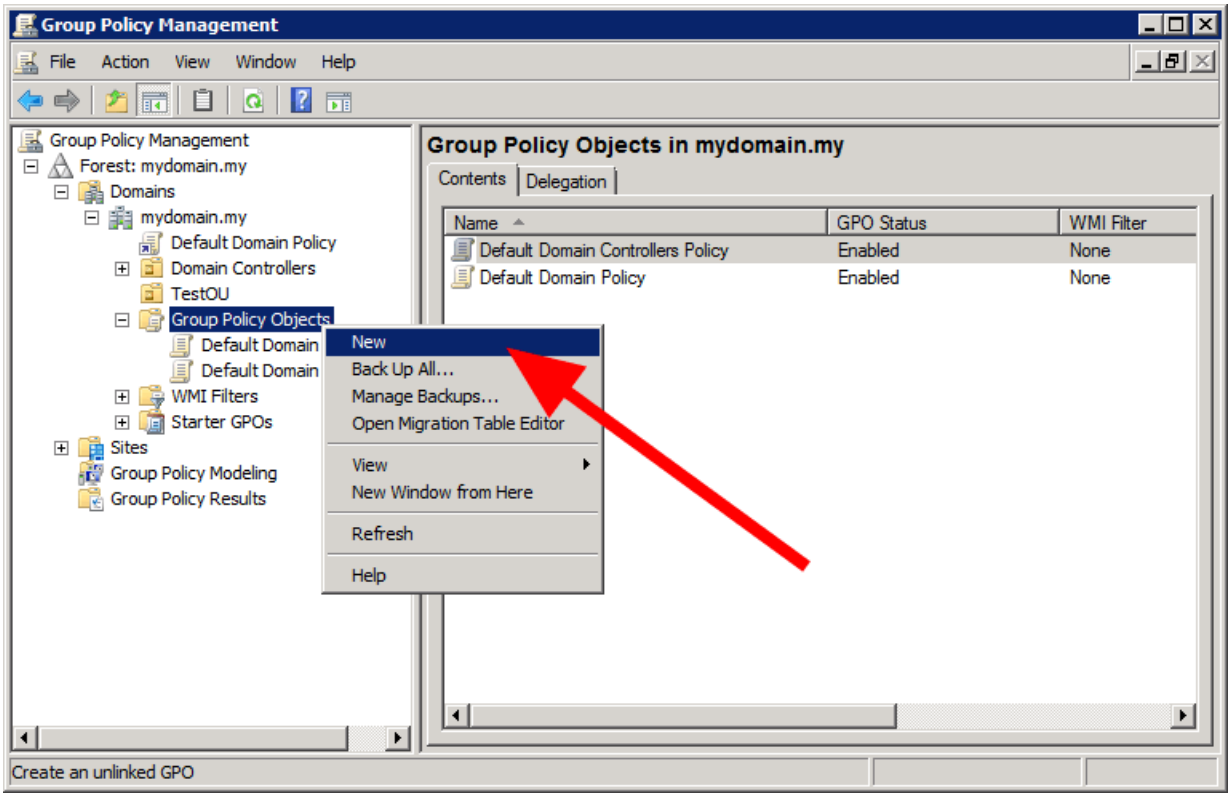
3.7.3.4. Способ 3. Установка через Active Directory

С помощью службы Microsoft Active Directory можно произвести автоматическую удаленную установку клиентской части на группу компьютеров. Для выполнения процедуры установки необходимо обладать правами администратора домена, на компьютеры которого необходимо установить клиента. Также необходимо иметь доступный на чтение сетевой ресурс (Shared Folder).

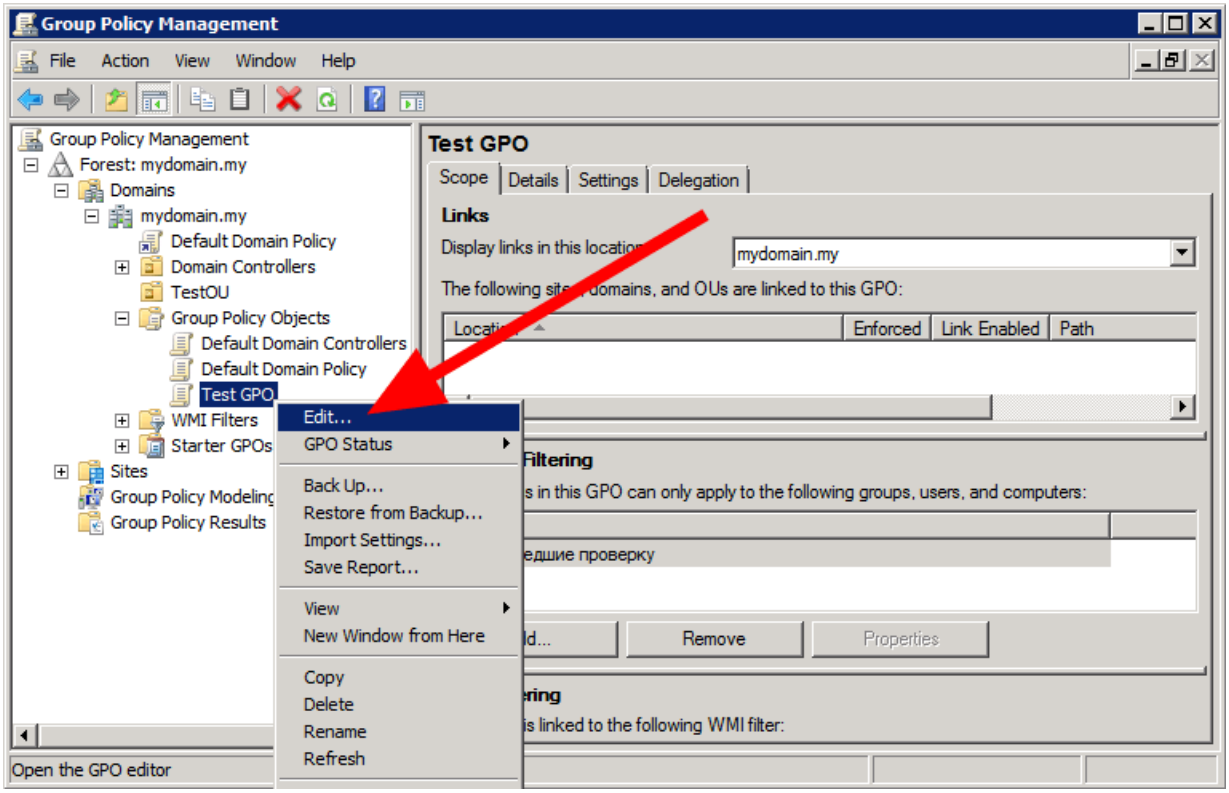
Запустите установщик, выбрав режим "Удаленная установка клиента". В мастере удаленной установки перейдите к способу 3.

Далее на примере будет показано создание GPO ("Test GPO"), установка в этом объекте msi-пакетов и adm-шаблона, а также линкование этого GPO к OU ("TestOU") с компьютерами, для которых требуется первоначально развернуть клиентов.

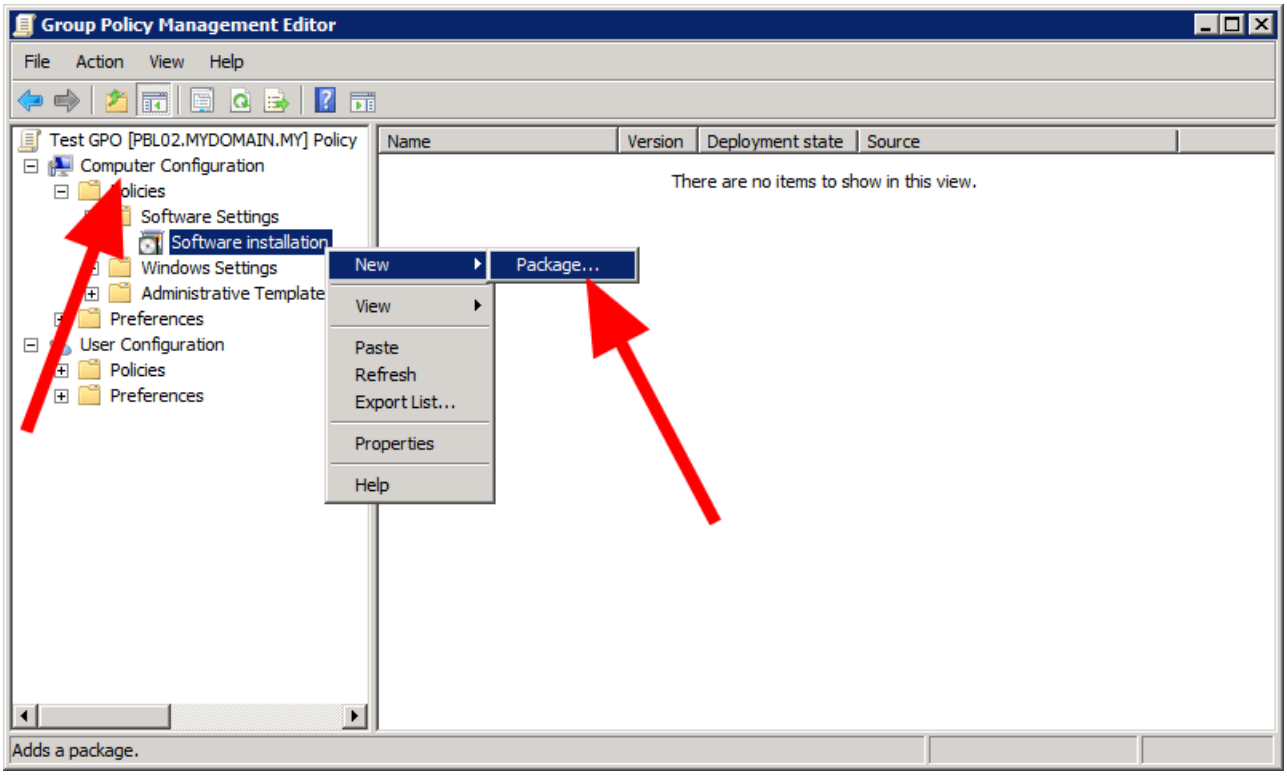
Создаем новый объект GPO ("Test GPO"):



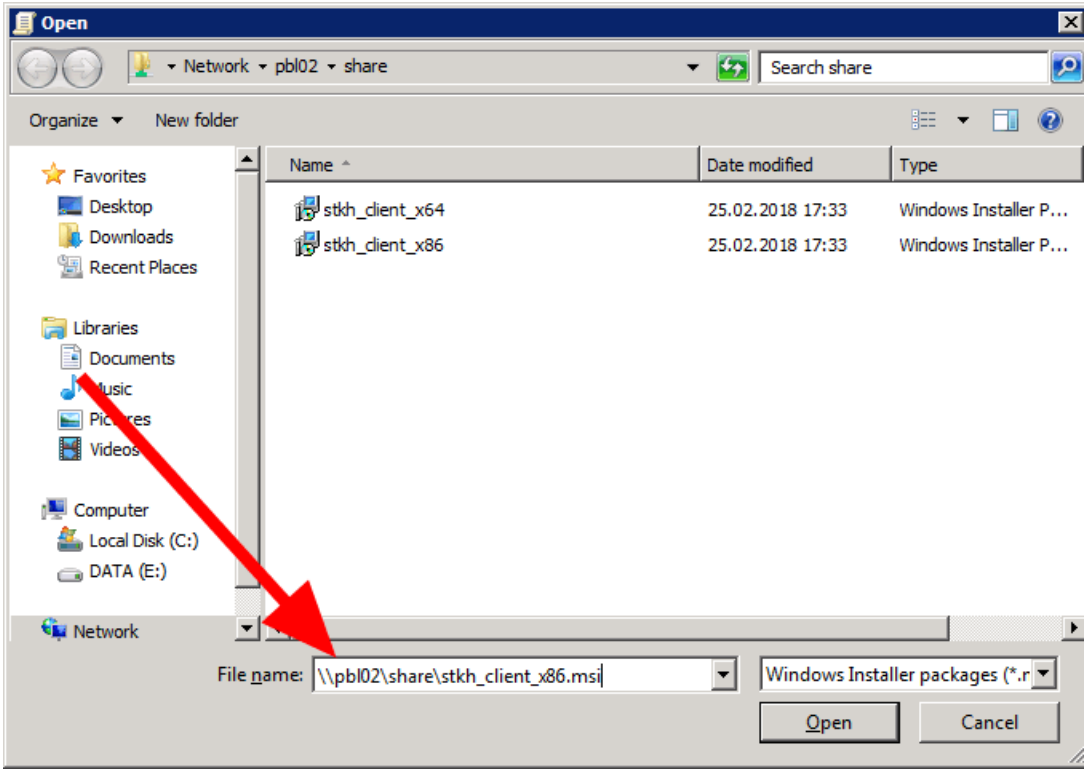
Редактируем созданный объект:



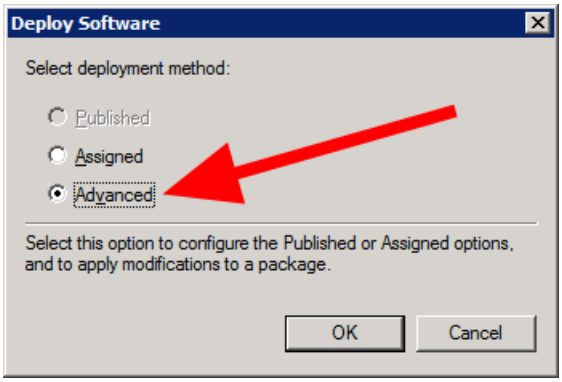
Для **Computer Configuration** добавляем msi-пакет:



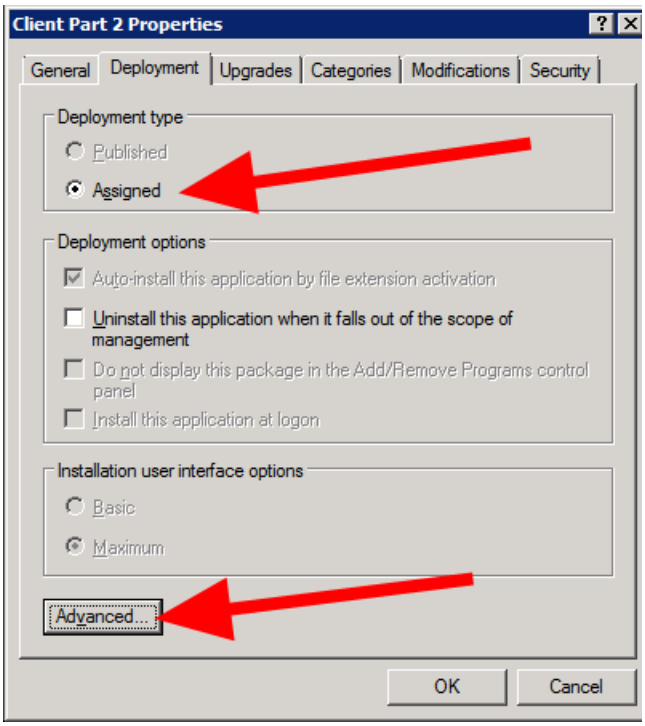
Выбираем путь к msi (x86) обязательно через **сетевой путь**.
В эту сетевую папку нужно предварительно скопировать msi-пакеты и клиентские машины должны иметь доступ к этому пути:



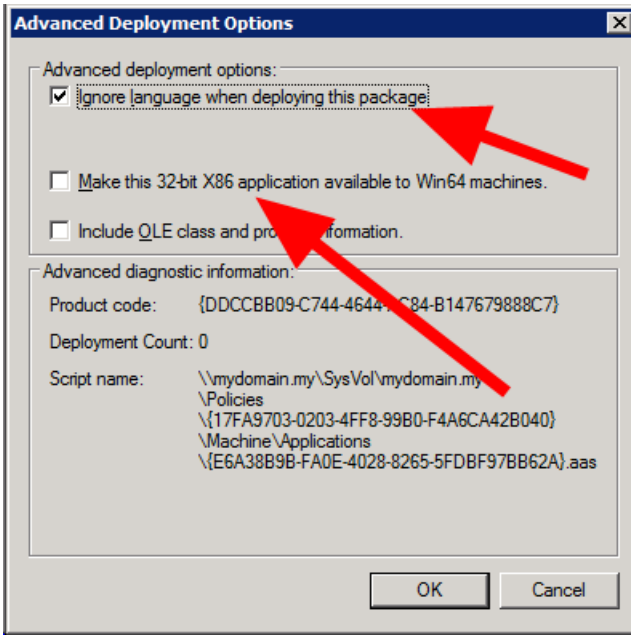
Выбор типа развертывания:



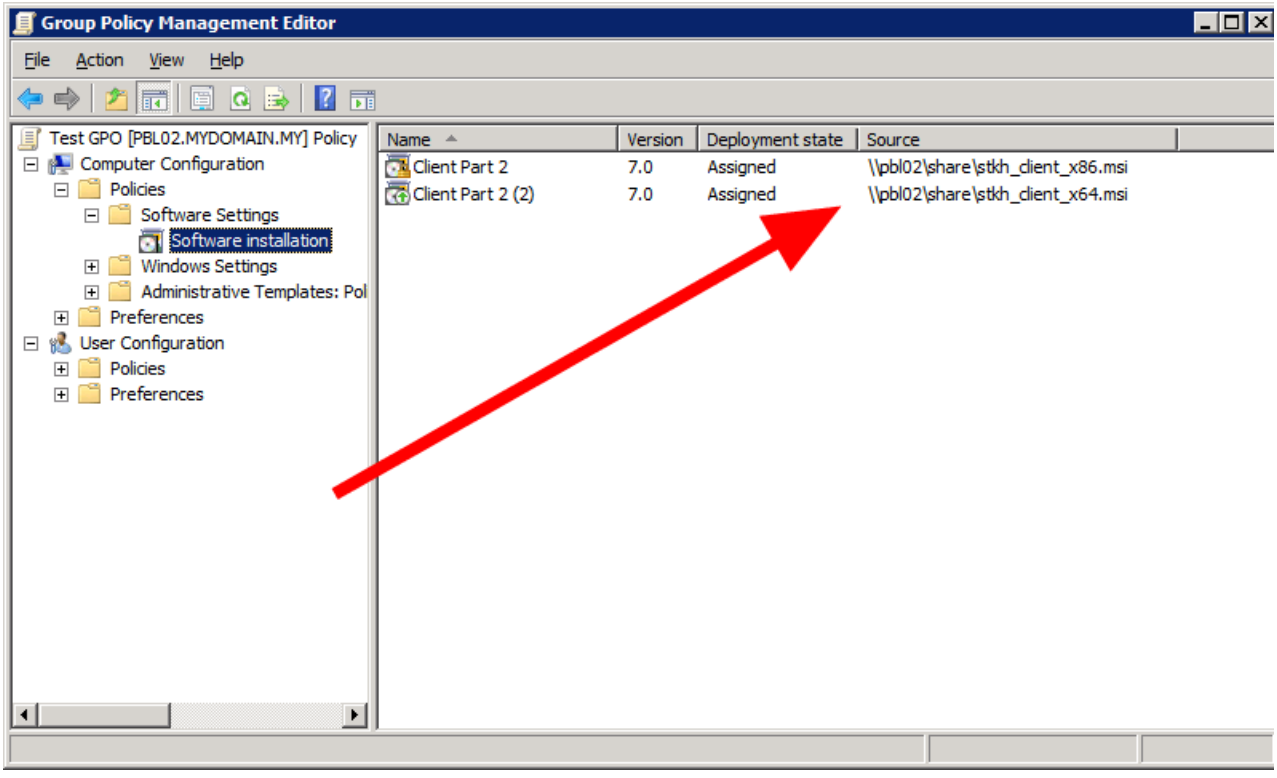
Запускаем расширенные опции:



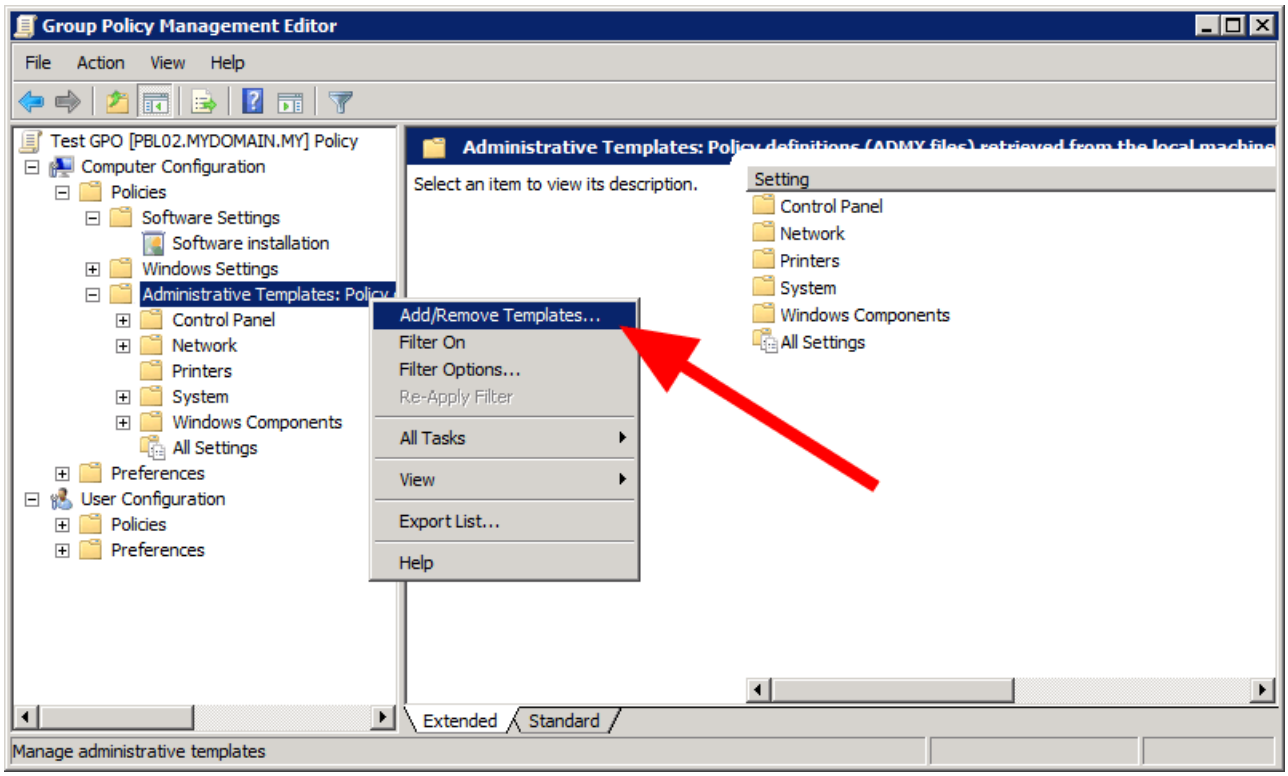
Изменяем флаги:



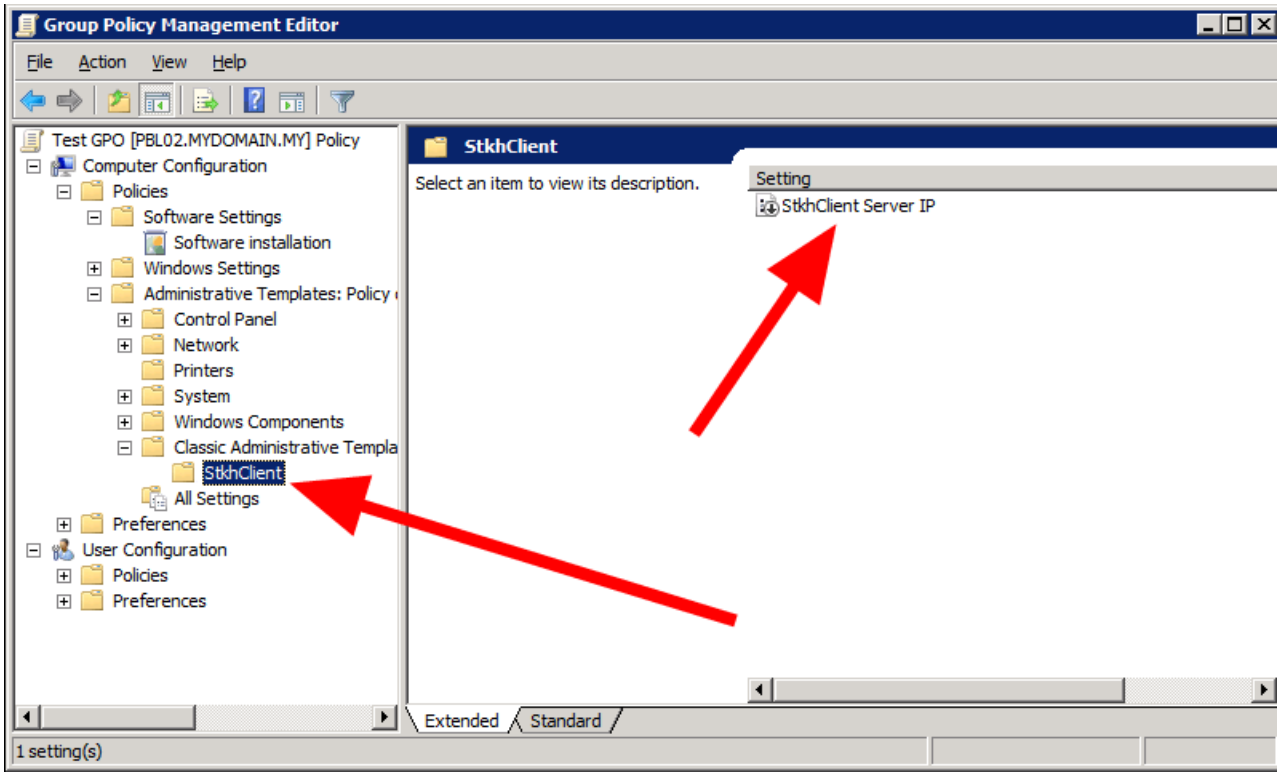
Все тоже самое для x64-пакета:



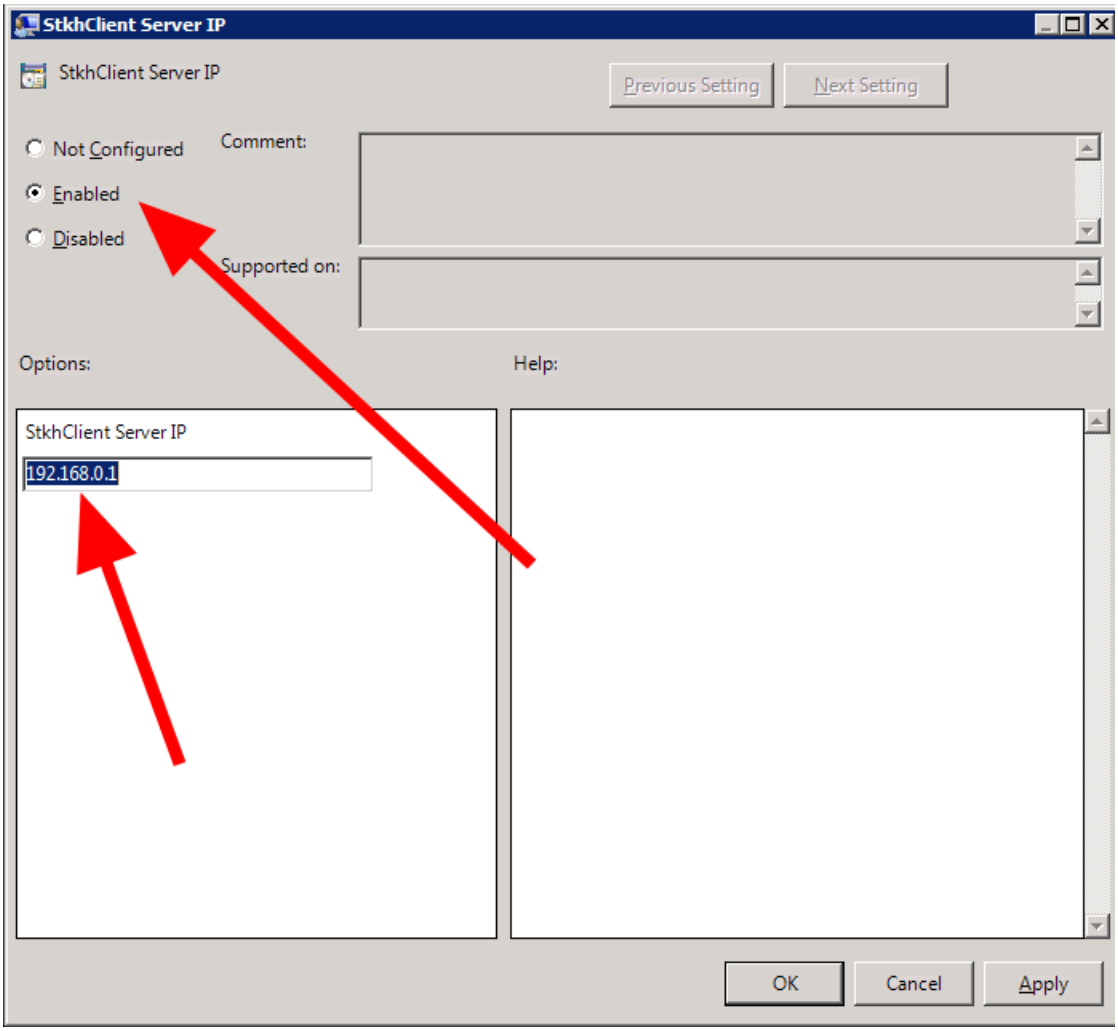
Добавляем шаблон из прилагаемого adm-файла:



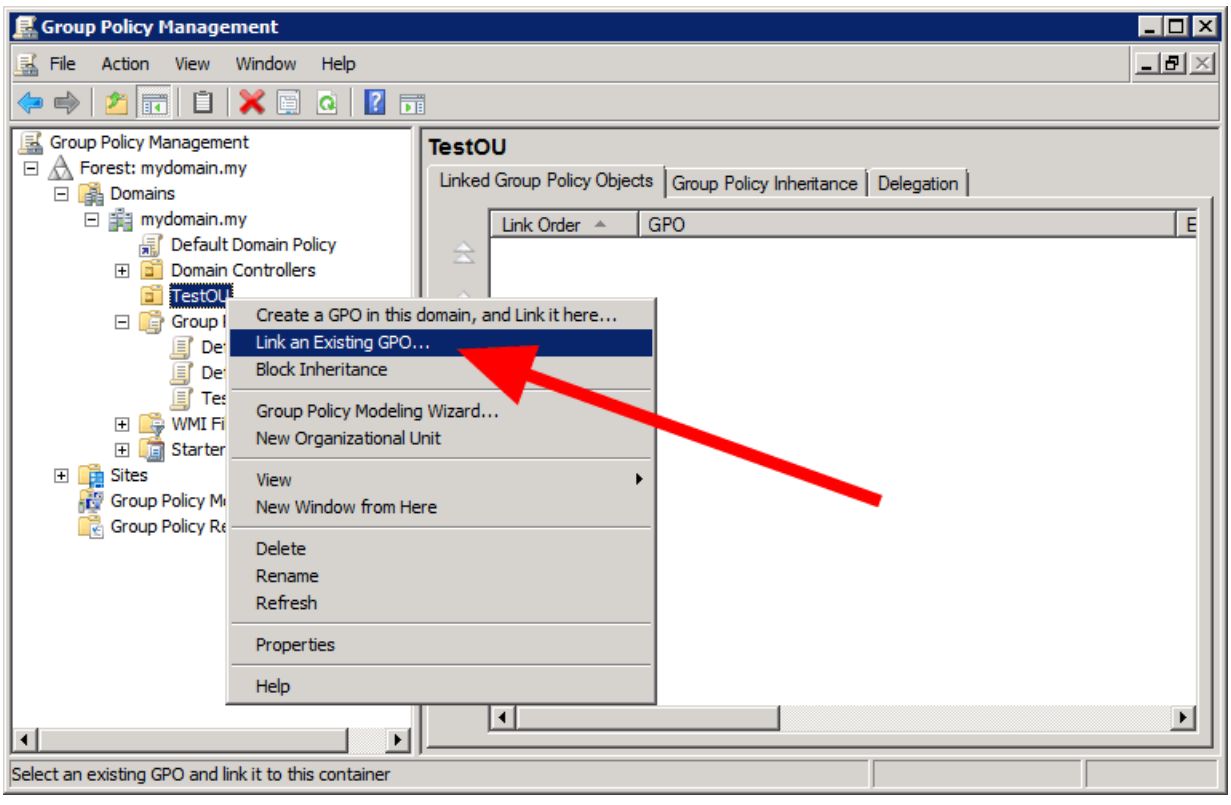
Редактируем добавленный шаблон:

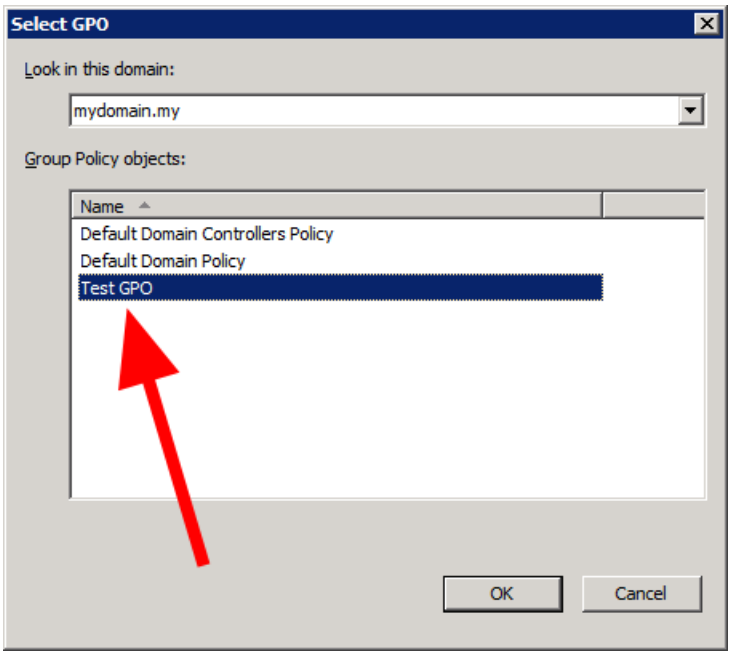


Устанавливаем IP/имя сервера для подключения клиентов:

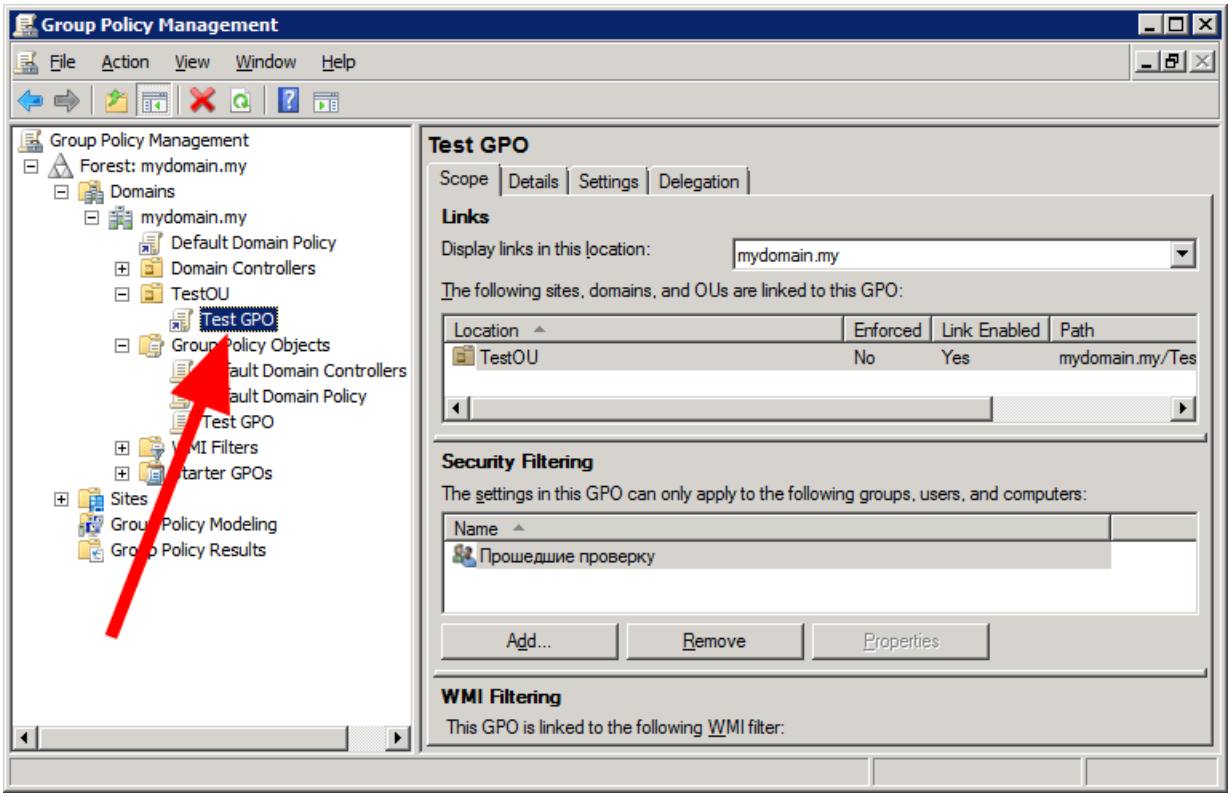


Линкуем созданный GPO к OU с компьютерами:





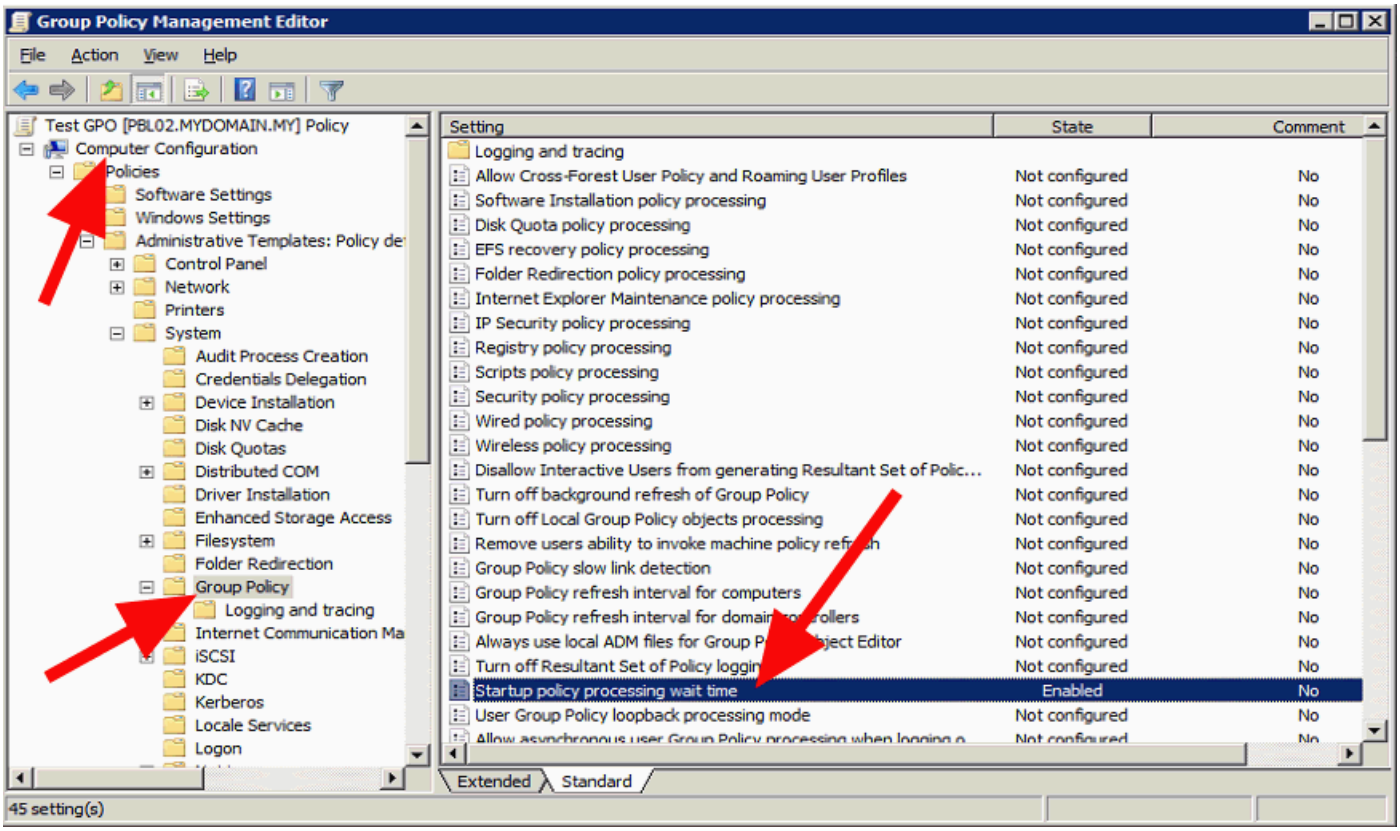
Настройка завершена:



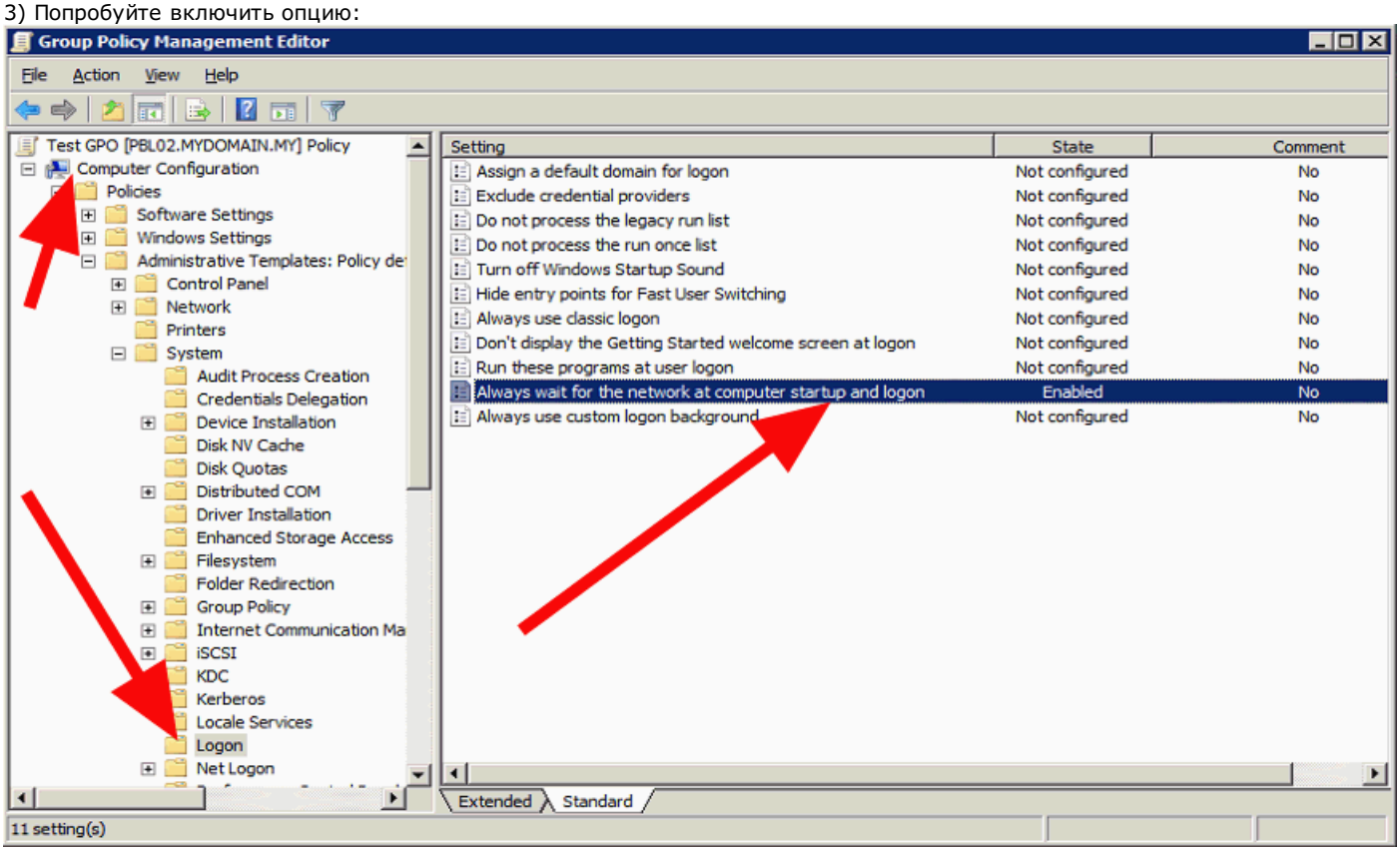
При следующей перезагрузке компьютеров, внесенных в организационную единицу, на них будет установлена и настроена клиентская часть комплекса.

Примечание: данный .msi-пакет не содержит информацию про обновления и uninstall, потому удаление и обновление осуществляйте только **средствами комплекса**, а не ActiveDirectory!

Если после перезагрузки **ничего не произошло**:
1) Попробуйте перезагрузить клиентскую машину еще раз.
2) Попробуйте увеличить время загрузки до 30 сек:



3) Попробуйте включить опцию:



4) На клиентской машине выполнить: **gpupdate /force**

См. также **"Автоматическое развертывание в среде Active Directory"**

3.7.3.5. Способ 4. Установка через командную строку

Запустите установщик, выбрав режим "Удаленная установка клиента". В мастере удаленной установки перейдите к способу 4.

Прилагаемый файл клиентской установки **inst_client.exe** можно запускать как **локально**, так и **удаленно**.
При локальном запуске без командной строки запустится обычная установка со всеми диалоговыми окнами (интерактивный режим).
Если запустить с командной строкой **-server <machine>**, то произойдет "тихая" установка клиента, который будет подключаться к серверу <machine>
Пример:
inst_client.exe -server 192.168.1.1

Обычно такой способ удаленной "тихой" установки можно использовать в **Microsoft System Center** или другом ПО, позволяющим удаленно запускать программы.

Важно! Если клиент уже установлен, то произойдет только изменение параметра **<machine>** для подключения к серверу.

Ниже приведены **коды возврата** выполнения команды:
0 - успешное выполнение;
1 - успешное выполнение, но клиент будет активирован после перезагрузки (иногда возможно только в WinXP);
-1 - неподдерживаемая старая ОС (Win2000/98);
-2 - необходимы права администратора;
-3 - пользователь отменил установку (только в интерактивном режиме);
-4 - установлен клиент версии 1.xx, необходимо сначала удалить его;
-5 - необходимо сначала выполнить перезагрузку, потом продолжить с установкой;
-6 - ошибка записи в файл;
-7 - в неинтерактивном режиме осуществлен запуск без командной строки.

Также через командную строку можно и **удалить клиента** с машины.
Удаление с сохранением отчетов: **inst_client.exe -uninstall_keep -key <KEY>**
Удаление также и отчетов: **inst_client.exe -uninstall_delete -key <KEY>**
Параметр **<KEY>** должен совпадать с ключем, который установлен на этой странице настроек.

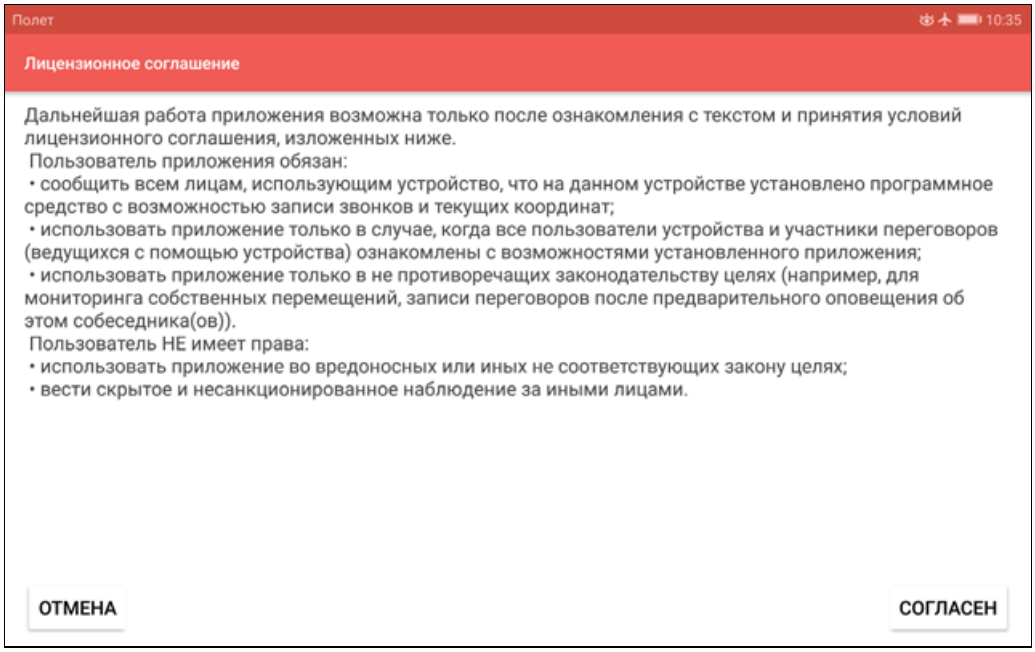
В случае удаления клиента доступны также дополнительные коды возврата:
-8 - нет связи с клиентом или клиент не установлен;
-9 - внутренняя ошибка;
-10 - ключ не установлен в настройках;
-11 - введенный ключ не совпадает с установленным в настройках.

3.7.4. Установка на смартфон (Android)

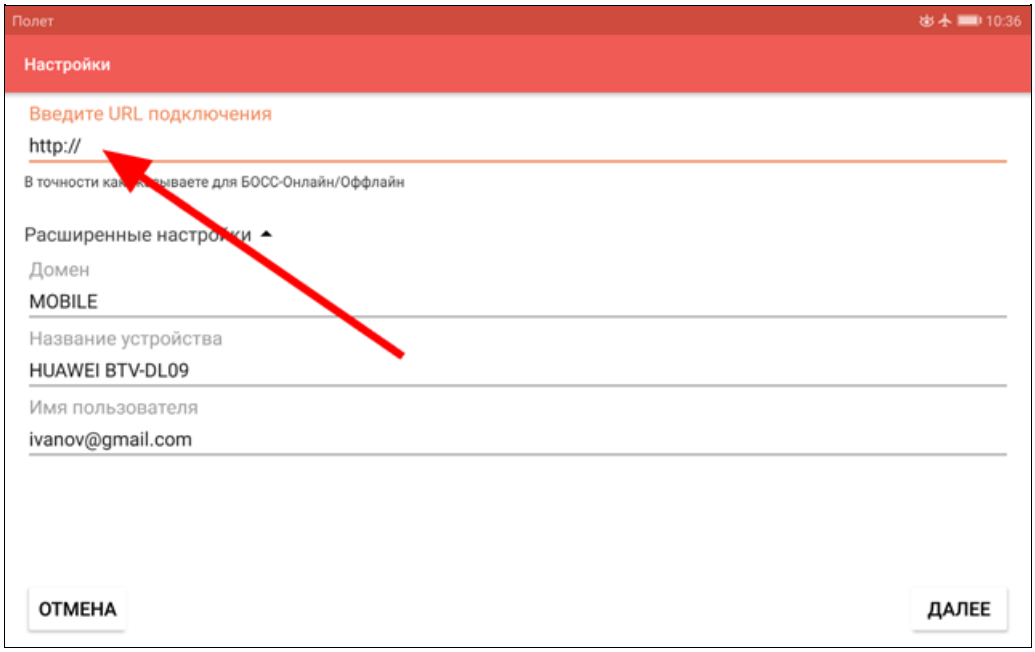
Установочный пакет (.apk) необходимо загрузить отсюда.
Перед установкой необходимо разрешить установку приложений **не из Маркета** (Расширенные настройки->Безопасность->Неизвестные источники).
Также перед установкой на устройство рекомендуется установить необходимые настройки на вкладке настроек "Мобильный клиент".

После установки и запуска откроется мастер настроек клиента.

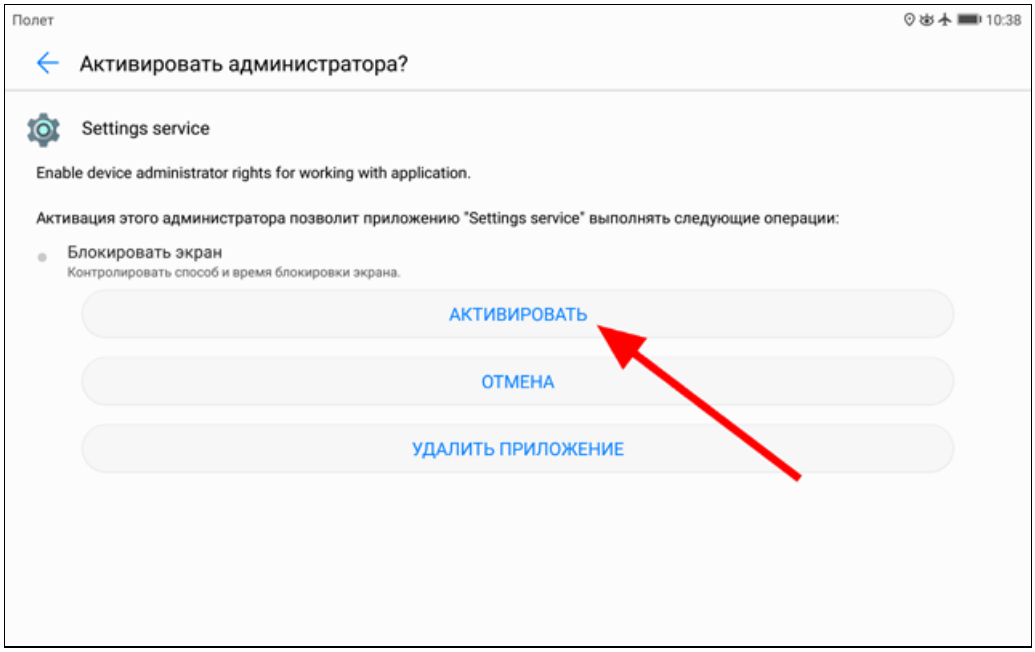
Необходимо прочесть и согласиться с условиями лицензионного соглашения использования:



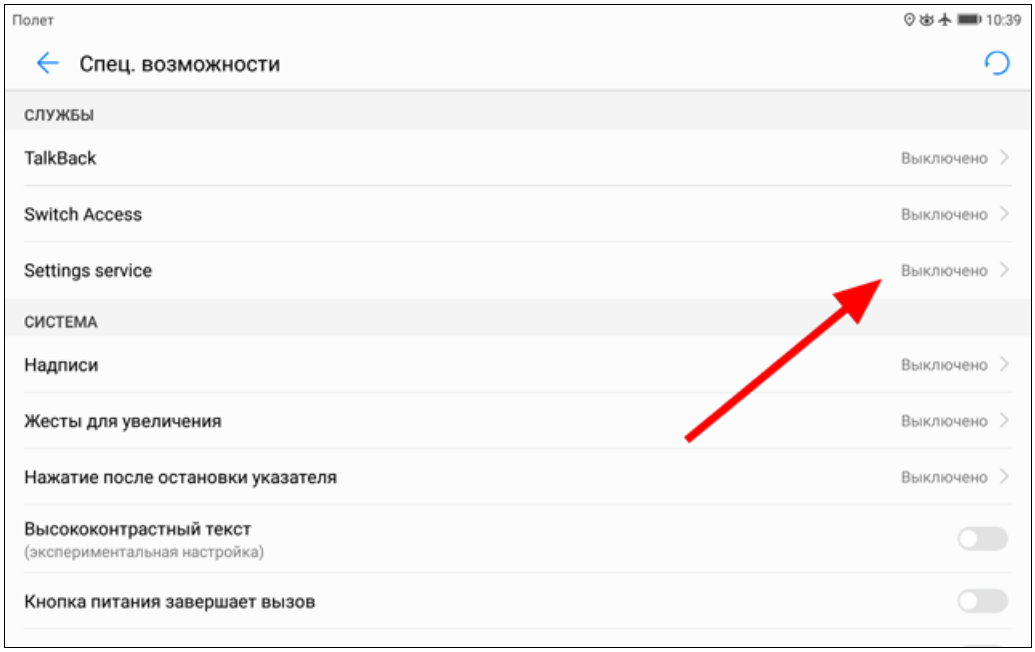
Далее нужно ввести URL подключения к серверу. Аналогично тому, как для входа в веб-интерфейс БОСС-Онлайн/Оффлайн.
Пример: **https://192.168.0.1/stkh**
Также можно изменить расширенные настройки (это идентификация устройства в отчетах БОСС-Оффлайн):



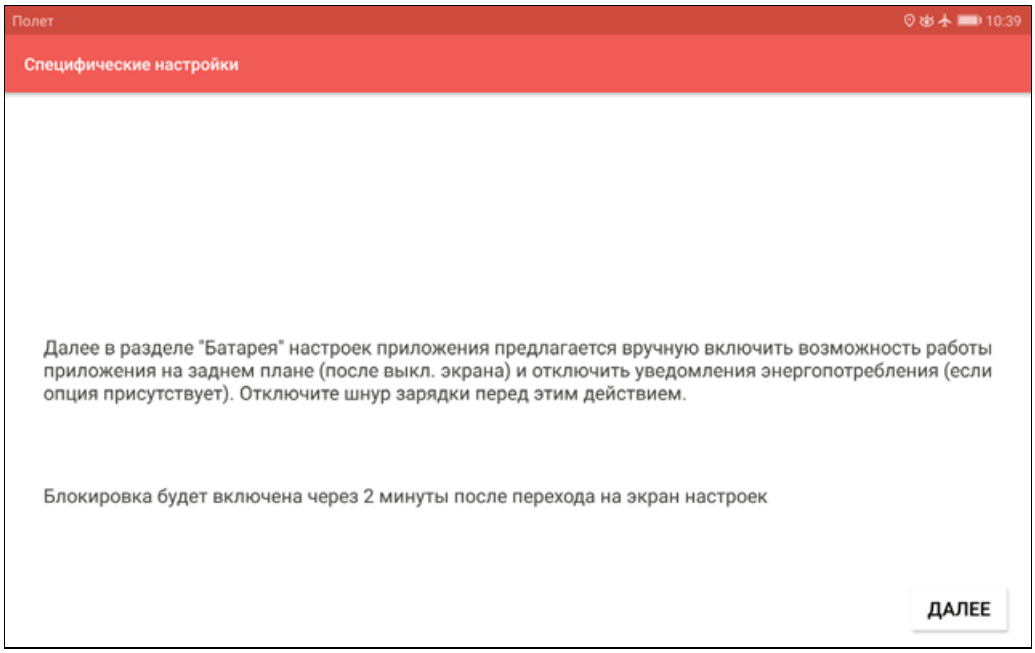
Активация администратора устройства:

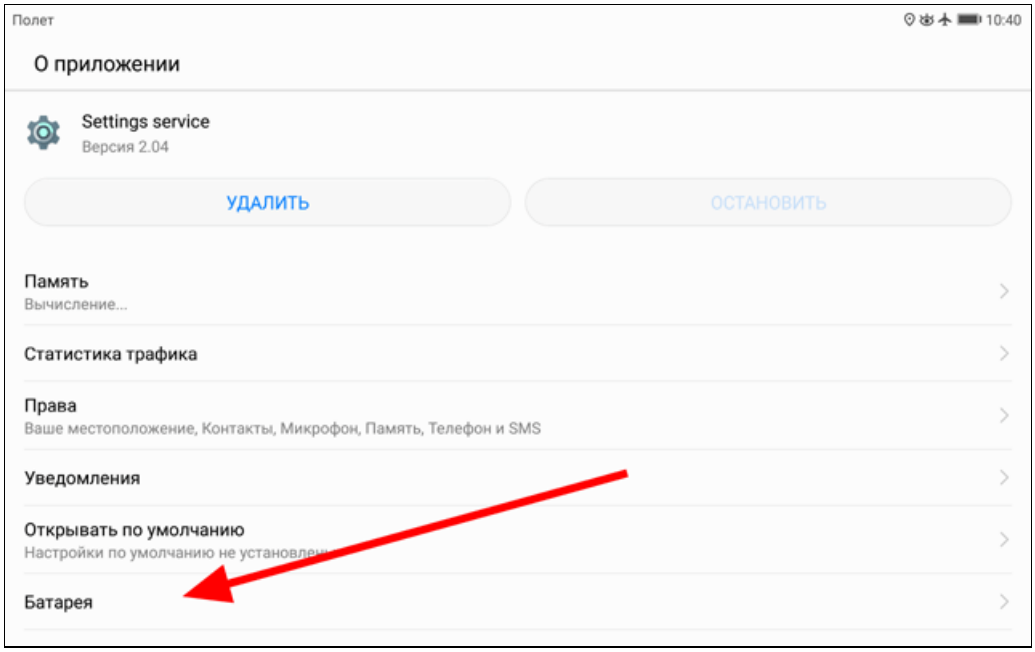


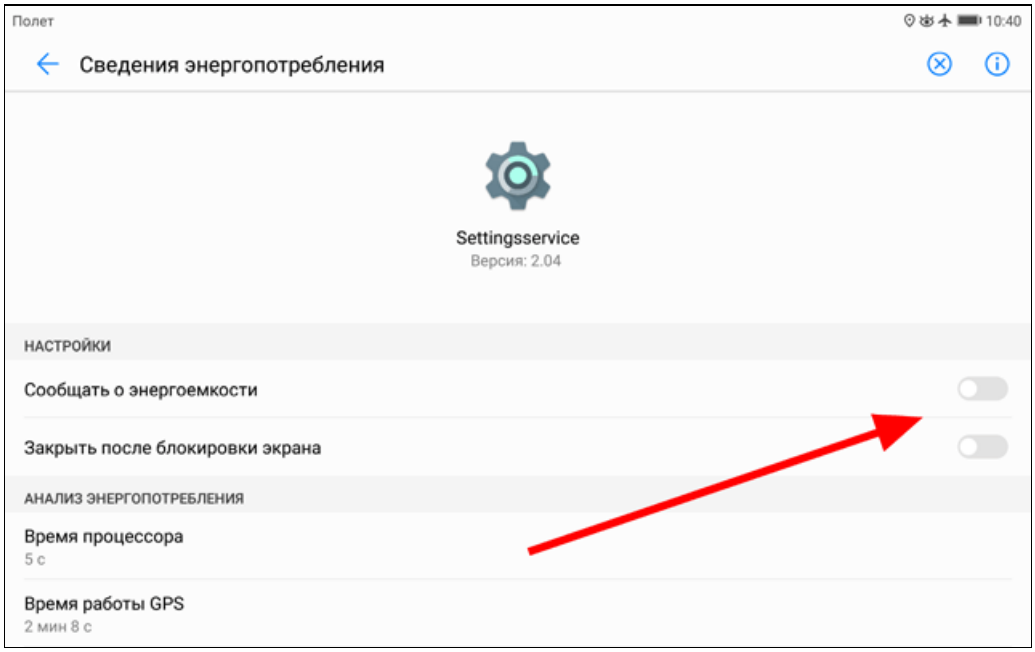
Включение сервиса:



После чего нажимаем **Back (Возврат)** на устройстве и попадаем на следующий экран мастера. Данный экран появится **только на некоторых устройствах (например, Huawei, Xiaomi)**. Цель данной настройки разрешить приложению работать в фоне, а также отключить уведомления об энергопотреблении:

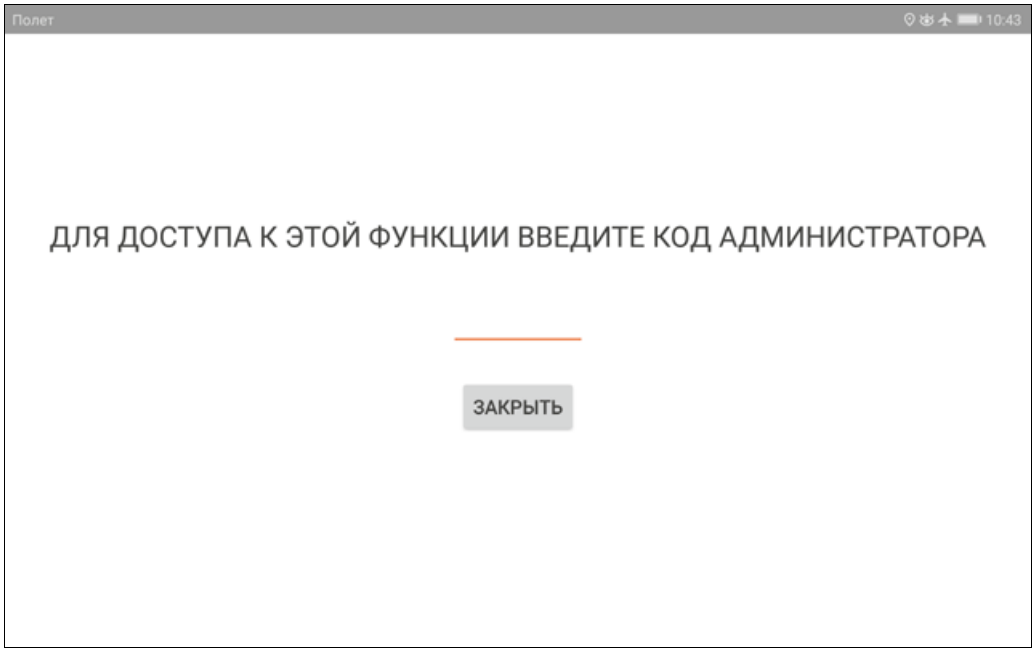

Полет
10:39
Специфические настройки
Далее в разделе "Батарея" настроек приложения предлагается вручную включить возможность работы приложения на заднем плане (после выкл. экрана) и отключить уведомления энергопотребления (если опция присутствует). Отключите шнур зарядки перед этим действием.
Блокировка будет включена через 2 минуты после перехода на экран настроек
ДАЛЕЕ


Полет
10:40
О приложении
Settings service
Версия 2.04
УДАЛИТЬ
ОСТАНОВИТЬ
Память
Вычисление...
Статистика трафика
Права
Ваше местоположение, Контакты, Микрофон, Память, Телефон и SMS
Уведомления
Открывать по умолчанию
Настройки по умолчанию не установлены
Батарея


Полет
10:40
Сведения энергопотребления
Settingsservice
Версия: 2.04
НАСТРОЙКИ
Сообщать о энергоемкости
Закрыть после блокировки экрана
АНАЛИЗ ЭНЕРГОПОТРЕБЛЕНИЯ
Время процессора
5 с
Время работы GPS
2 мин 8 с

Внимание! **Внешний вид окон и настроек может отличаться от показанного в разных устройствах!**

Теперь клиент **активен и работает**.
Следующие **2 минуты** он находится в **администраторском режиме** (в котором приложение можно удалить), а далее происходит переключение в режим пользователя, и при попытке удалить приложение или зайти на запрещенный экран появится запрос на ввод **пин-кода**, который настраивается в настройках "Мобильный клиент":



Важные особенности:
• для **изменения настроек** нужно удалить приложение и установить снова;
• для **удаления приложения** сначала нужно в настройках "Расширенные настройки->Безопасность->Администраторы устройства" убрать галочку напротив "Settings Service";
• для **обновления приложения** можно установить новый .apk поверх старой версии;
• если используется GPS-трекинг, то нужно включить **геолокацию** в настройках устройства;
• клиент подключается кратковременно к серверу только когда есть связь, поэтому в **БОСС-Онлайн он виден не будет!**;
• при отсутствии связи с сервером данные мониторинга **накапливаются локально** на устройстве;
• в **Android 7/8+** очень ограничена работа приложений в фоне, поэтому связь с сервером осуществляется не чаще чем **один раз в 15 минут** (это следует учесть при построении отчетов и изменении настроек);
• перехват посещенных URL сайтов осуществляется только в браузерах **Интернет** и **Chrome**;
• в отчет **"Чаты/Звонки"** попадают только SMS и GSM-переговоры, остальная активность - в отчет **"Программы"**;
• после установки и настройки приложения его иконка вьывает стандартные настройки системы.

3.8. Шаг 5. Наблюдение для начальника

Модуль начальника разделен на два: **"БОСС-Онлайн"** и **"БОСС-Оффлайн"**. Первый предназначен для наблюдения за включенными машинами и пользователями в реальном времени, а также выполнения ряда администраторских функций. Второй - для просмотра отчетов по пользователям из базы данных. Причем, в данном случае не требуется включения клиентских машин.

Фактически **"БОСС-Онлайн"** и **"БОСС-Оффлайн"** представлены в виде веб-интерфейсов, т.е. для наблюдения и просмотра отчетов не нужно устанавливать дополнительного ПО, а нужно просто запустить любой браузер с любого компьютера в сети и осуществить переход по определенному веб-адресу (см. ниже).
Однако, **"БОСС-Онлайн"** включает в себя также и **внешний модуль**, который позволяет расширить функционал наблюдения.

На любом компьютере запускаете любой браузер и вводите в адресной строке:
http://<DNS_имя_или_IP_сервера>/stkh
Примеры:
http://localhost/stkh (**если сервер СТАХАНОВЕЦ на этой же машине**)
http://server/stkh
http://mycompany.org/stkh
http://95.135.21.16/stkh

Однако, если инстанция сервера отлична от инстанции по умолчанию, то путь имеет вид **/stkh.X**, где **X** - номер инстанции.
Пример:
http://remoteserver/stkh.2 (подключение к инстанции номер 2 сервера)

Если используется нестандартный порт веб-сервера (не путать с портом сервера СТАХАНОВЕЦ!), то его необходимо указать после двоеточия.
Пример:
http://myserver:81/stkh (подключение к **порту 81**, а не стандартному 80)

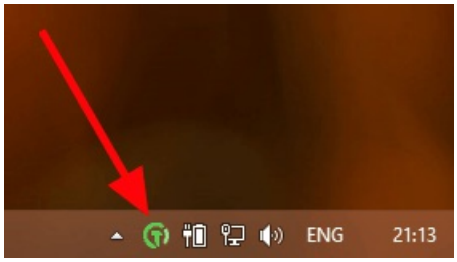
Внимание! На некоторых мобильных устройствах (смартфонах) необходимо вводить IP-адрес, а не имя сервера (если он в локальной сети).

О том, как настроить **удаленное наблюдение через Интернет**, см. здесь
О том, как настроить доступ по **https: через SSL** см. здесь

Рассмотрим более подробно **"БОСС-Онлайн"**.
Сразу после запуска **"БОСС-Онлайн"** будет предложено сделать вход в базу данных для идентификации логина начальника и его прав (которые ранее ему задал администратор в программе администратора).
По истечении 1-2 секунд произойдет получение списка активных машин с сервера (в случае успешного соединения с сервером и наличия активных машин в сети).
Под активной машиной подразумевается машина с установленной на ней клиентской частью.
При этом следует разделять понятия "пользователь" и "машина":
Машины в списке - компьютеры с установленными клиентскими частями комплекса ПО;
Пользователи в списке - загруженные пользователи Windows.
Таким образом, на одной машине может быть сразу несколько пользователей (например, в случае **терминального сервера** или режима **FastUserSwitch**)
Естественно и действия для пользователей и машин отличаются. Так, например, можно обновить клиентское ПО на **машине**, а получить снимок экрана **пользователя**!
Машины и пользователи, которые в данный момент не в сети или с ними нет связи (но ранее была), будут отображаться **красным цветом в соотв. вкладке**.

Для некоторых функций в БОСС-Онлайн необходим запуск внешнего модуля. При вызове этих функций будет предложено **скачать и запустить вспомогательный модуль БОСС-Онлайн для Windows**.
После запуска иконка модуля появится на **рабочем столе** и в **трее**.
Мигающая иконка в трее говорит об ошибке соединения с сервером комплекса. Текст ошибки можно прочесть если навести указатель мыши на иконку.
По **правому клику** на иконке в трее доступно **меню настроек**.

Внимание! Иконка в трее может не показываться из-за настроек таскбара "Не показывать редко-используемые иконки".



Теперь перейдем к рассмотрению **"БОСС-Оффлайн"**.
"БОСС-Оффлайн" предназначен для просмотра отчетов о действиях пользователей из базы данных. Программа не

требует того, чтобы машины были включены в текущий момент. Более того, есть возможность просмотра данных отчетов **из удаленного места** (например, из дому) если технически это разрешено сетевой инфраструктурой и настроено должным образом сетевым администратором.

Следует отметить, что данные в базу записываются **не мгновенно**, а спустя некоторое время (около 10 мин), потому сразу после установки ПО рассчитывать на их моментальное появление не стоит.

4. Удаление комплекса:

4.1. Удаление (деинсталляция) комплекса

Удаление необходимо производить в **обратном порядке** установки.

1. Выполнить удаление всех клиентских частей через **"БОСС-Онлайн"** (см. также).
2. Удалить и программу администратора на администраторской машине.
3. Удалить сервер СТАХАНОВЕЦ таким же способом.

Следует заметить, что все настройки **сохранятся** даже после удаления.
Это касается также и **базы данных** СТАХАНОВЕЦ (информация только для MSSQL Server).
При желании вы можете удалить и SQL-сервер (через "Панель управления->Установка и удаление программ"), однако сам файл БД СТАХАНОВЕЦ останется (информация только для MSSQL Server), чтобы впоследствии можно было его снова подключить к базе. Если пожелаете его удалить, то сделать это нужно будет вручную из папки SQL-сервера (обычно это "\Microsoft SQL Server\MSSQL\Data\stkh.*") (информация только для MSSQL Server)
Для MySQL: останутся файлы БД после его удаления или нет зависит от конкретной версии сервера.

5. Обновление комплекса:

5.1. Обновление комплекса

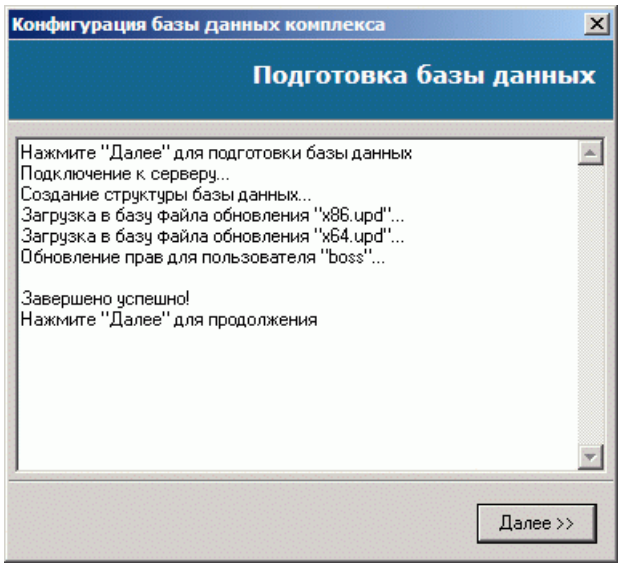
Обновление программ **администратора** и **сервера** необходимо производить **вручную** (т.е. установить новую версию поверх имеющейся), однако для обновления **клиентских машин** нужно использовать обновление через **"БОСС-Онлайн"** или опцию автоматического обновления клиентов.

Последовательность действий:

1. Скачать с сайта дистрибутив последней **демо**-версии (**установку "в один клик" использовать нельзя!**)

2. Рекомендуется остановить службу сервера комплекса. Сделать это можно через меню Пуск->Программы->СТАХАНОВЕЦ Сервер->"Остановить сервер" (выполнять команду нужно от имени администратора!).

3. Выполнить установку программы **администратора** поверх имеющейся версии. При этом **НЕЛЬЗЯ** отменять запуск утилиты конфигурации базы данных, которая автоматически запускается в ходе установки.



4. Снова запустить дистрибутив установщика и выбрать **установку сервера**, обновить сервер поверх имеющейся версии.

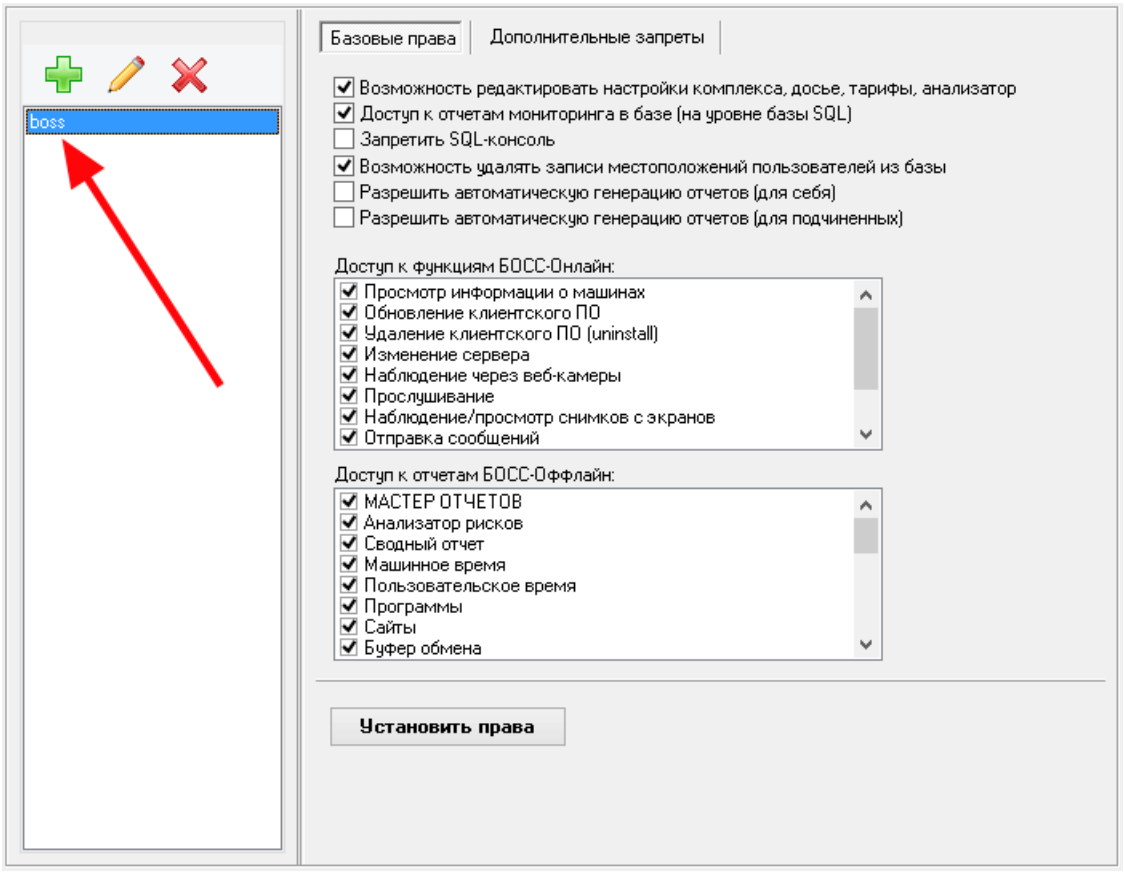
5. Через **"БОСС-Онлайн"** выполнить обновление всех **клиентских машин** по команде **"Обновить клиентское ПО"**. Если включена опция **автоматического обновления** клиентов (по умолчанию она **включена**), то данное действие выполнится автоматически в течение 1-2 часов. Активация новой версии клиента происходит только **после перезагрузки** клиентской машины!
Посмотреть текущую версию клиентской части можно через функцию БОСС-Онлайн **"Общие сведения"**.

6. Глобальные настройки:

6.1. Пользователи базы

На этой странице можно добавлять начальников (**хотя бы один обязателен!**), а также дополнительных администраторов (при необходимости). Между собой они отличаются только правами доступа. Добавлять и изменять права можно только при входе под **администратором базы данных!**
Добавление представляет собой создание нового пользователя **в SQL-базе** и назначение ему прав.
Важное замечание: если какой-то пользователь уже есть в SQL-базе и вы хотите, чтобы он смог работать с базой СТАХАНОВЕЦ, то его необходимо **обязательно** добавить на этой странице, т.к. просто того, что он есть в базе SQL **недостаточно** для полноценной работы!
Для **MSSQL** возможно также добавление **учетных записей Windows** - укажите пользователя в формате **DOMAIN\username** (домен без точки в сокращенном виде).
Созданные здесь начальники и дополнительные администраторы также могут входить в программу глобальных настроек, однако не смогут добавлять/удалять пользователей и устанавливать их права. Это может делать только администратор базы данных!

Пример создания начальника "boss":



Наиболее важные опции в правах начальника:

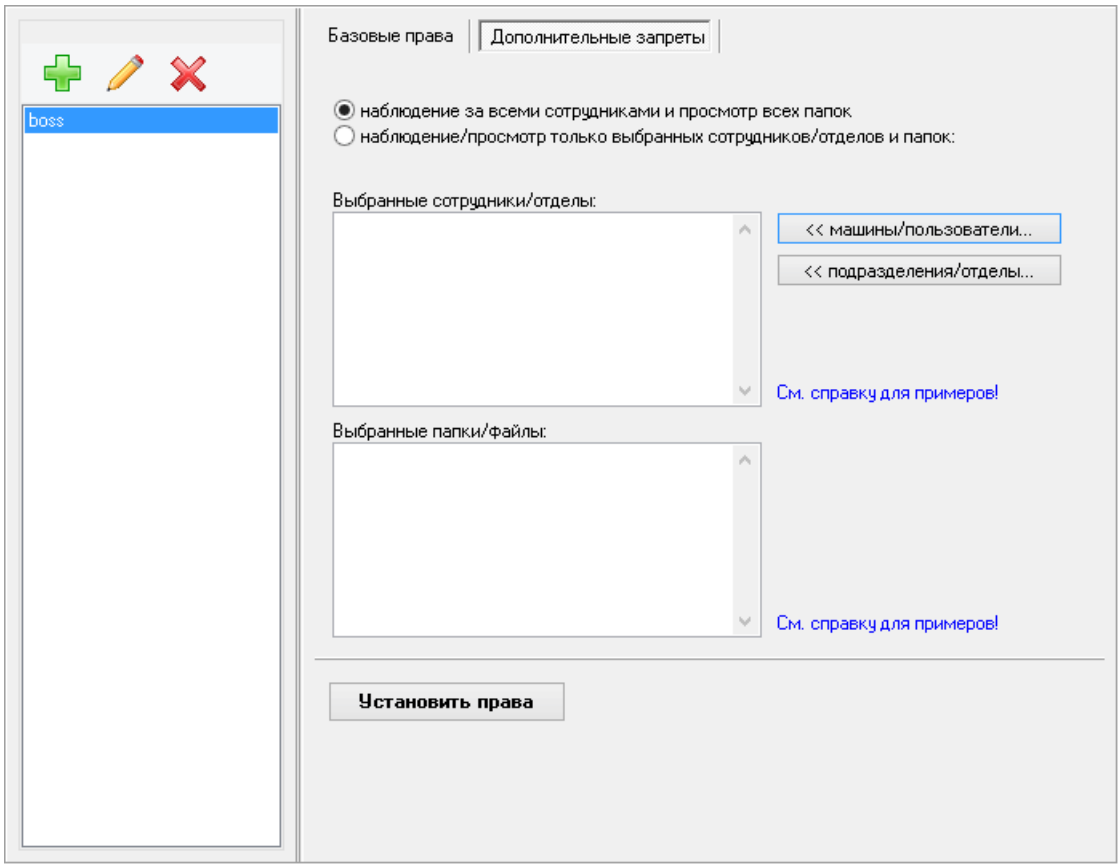
Возможность удалять записи местоположений пользователей из базы
Разрешить или запретить работу на странице "Списки пользователей".

Разрешить автоматическую генерацию отчетов (для себя)
Разрешает автогенерацию отчетов по своим подчиненным с отправкой отчетов себе (или сохранением в папку).
Более подробно описано в справке описания серверных настроек "Генератор отчетов".

Разрешить автоматическую генерацию отчетов (для подчиненных)
Разрешает автогенерацию отчетов по своим подчиненным с отправкой отчетов самим подчиненным.
Более подробно описано в справке описания серверных настроек "Генератор отчетов".

Разрешить команды к серверу через Telegram
Разрешает отправлять данному начальнику команды управления на сервер через мессенджер Telegram. Более подробно см. здесь

Отдельно рассмотрим "Дополнительные запреты" в разделе назначения прав для пользователей базы:



По умолчанию созданный пользователь базы может наблюдать в режимах онлайн/оффлайн за всеми сотрудниками/отделами и смотреть все папки через БОСС-Оффлайн. Однако бывает полезно назначить для каждого пользователя базы (начальника) каких-то конкретных сотрудников или отделы для наблюдения. В этом случае можно выбрать такие отделы (и при необходимости сотрудников), аналогично и с папками при просмотре через БОСС-Оффлайн.

Для выбора сотрудников можно воспользоваться кнопкой "машины/пользователи" (пока в базу не поступили данные от сотрудников, данный список будет пуст!) или же вводить данные вручную.
Для выбора отделов - кнопкой "подразделения/отделы" (создается структура компании в соотв. пункте глобальных настроек).
Примечание: права на отдел распространяются также рекурсивно на все его дочерние отделы.
Примечание: корневой отдел (название компании) не указывается в иерархическом пути отдела.
Примечание: если добавлен отдел, то нет смысла добавлять отдельно всех пользователей/компьютеры внутри него.
Каждая запись в списке должна начинаться с **новой строки**!
Формат записи для компьютера: **КОМПЬЮТЕР.ДОМЕН** (для организаций с доменами) или **КОМПЬЮТЕР.РАБОЧАЯ_ГРУППА** (для организаций с рабочими группами).
Важно! Домен должен указываться в **полном формате**!
Важно! Если нет домена, но используется DNS-суффикс подключения, то нужно указывать его. В общем случае компьютеры должны указываться так, как отображаются в списке компьютеров в БОСС-Оффлайн.
Формат записи для пользователя: **ДОМЕН\ПОЛЬЗОВАТЕЛЬ** (для доменных пользователей) или **КОМПЬЮТЕР\ПОЛЬЗОВАТЕЛЬ** (для локальных пользователей).
Важно! Домен должен указываться в **сокращенном формате (без точек)**!

Для выбора разрешенных папок/файлов достаточно указывать фрагменты пути к файлу (каждый фрагмент с новой строки). При этом использование масок "*" и "?" не разрешается! Вместо масок нужно просто не указывать ту или иную часть пути.
Примеры фрагментов:
_PC1\PC1_Ivanov\
\Department1_
Таким образом, если при просмотре файлов через БОСС-Оффлайн полный путь к файлу содержит хотя бы один фрагмент данного списка, то данный файл будет показан в отчете.

После настройки прав необходимо нажать кнопку **"Установить права"**

6.2. Настройки комплекса:

6.2.1. Общее описание настроек

Все настройки комплекса делятся на **серверные** и **клиентские**.
Серверные используются самим сервером.
Клиентские используются клиентскими машинами и пользователями, эти настройки они получают от сервера при старте и в ходе работы. Если с сервером временно отсутствует связь, то будут использоваться предыдущие настройки, кот. сохраняются в локальном кэше клиентских машин.
Изменения настроек вступают в силу через 1-3 минуты.
Узнать, какие настройки используются в данный момент можно через функцию **БОСС-Онлайн "Общие сведения"**.

Также **клиентские** настройки делятся на: **"для компьютеров"**, **"для пользователей"** и **"группы"**.
Для компьютеров - настройки, которые воспринимаются компьютерами, но не пользователями! Т.к. на одном компьютере могут работать несколько пользователей (одновременно как в терминальном сервере или по очереди).
Для пользователей - настройки, которые воспринимаются отдельными пользователями компьютеров, но не самими компьютерами.
Чтобы понять эту разницу, можно просто заглянуть в сами настройки и увидеть, чем они отличаются.
Группы нужно использовать, если вы **не хотите**, чтобы клиентские настройки **были одинаковыми** для всех компьютеров/пользователей и необходимо реализовать возможность установки своих индивидуальных настроек для определенных групп пользователей/компьютеров. В этом случае необходимо создать профили настроек, а потом сопоставить группы с этими профилями. Для создания профилей необходимо вызвать **выпадающее меню** рядом с кнопками "Для компьютеров", "Для пользователей".
Внимание! Если в вашем случае настройки для всех компьютеров и пользователей должны быть **одни и те же**, то создавать профили и группы **не нужно**!

6.2.2. Серверные настройки:

6.2.2.1. Общие настройки

Наиболее важные опции на этой вкладке:

Хранить отчеты не более N-дней
Укажите ретроспективу хранения пользовательских отчетов в базе данных и в папках. Не указывайте слишком большое значение, чтобы не занимать много места на SQL-сервере и диске.

Вести отчеты пользователей _LOGOFF_ (состояние завершенного сеанса)
Если на компьютере не выполнен вход ни для одного пользователя, то в БОСС-Онлайн можно увидеть пользователя с именем **_LOGOFF_**.
При необходимости можно разрешить накапливать отчеты таких пользователей.

6.2.2.2. Отложенный мониторинг

Отложенный мониторинг имеет смысл использовать для экономии сетевого трафика клиент-сервер, а также снижения нагрузки на сервер комплекса и базу данных при большом количестве клиентских подключений к серверу. При включении режима данные мониторинга накапливаются локально на клиентских машинах и не передаются на сервер если отчеты по данному компьютеру/пользователю не строились более N-дней (параметр **"Условие включения режима"**). Сам способ построения отчетов не играет роли - ручной или через автоматическую генерацию отчетов. Если отчеты строятся постоянно по конкретному пользователю/компьютеру чаще чем раз в N-дней, то работа не будет отличаться от обычного режима. Таким образом, "неинтересные" в данный момент для наблюдения пользователи не будут нагружать сеть и базу своими данными (ретроспектива локального хранения на машинах и пр. опции настраиваются на вкладке настроек для компьютеров **"Локальное хранилище"**). Если же построить отчет по пользователю, находящемуся в отложенном режиме работы, то сразу данных в базе, естественно, не будет и отчет будет пустым. Однако, спустя 1-2 минуты с этой машины накопленные данные начнут передаваться на сервер пока не передадутся все. Т.е. пользователь перейдет в обычный режим работы.
Посмотреть текущий размер локального хранилища машины можно через функцию БОСС-Онлайн **"Общие сведения"**. Также через БОСС-Онлайн можно удалить локальное хранилище.
Также существует возможность автоматической установки флагов отложенного мониторинга для тех или иных пользователей в ходе синхронизации с Active Directory. Более подробно описано в разделе справки **"Синхронизация с Active Directory"**.
Параметр настроек **"Для новых компьютеров/пользователей"** определяет, в каком режиме начинать работу клиенту, который подключен только что и является новым - в отложенном или обычном.
Внимание! Часто существует необходимость, чтобы для группы пользователей/компьютеров не применялся отложенный режим при общем включении режима. В этом случае для данной группы пользователей/компьютеров необходимо установить флажки "Никогда не переходить в отложенный режим работы" на вкладках "Общие настройки" для пользователей/компьютеров соотв.

6.2.2.3. Мониторинг - Снимки экранов

Наиболее важные опции на этой вкладке:

Сохранять снимки в папке
Укажите папку на сервере, куда будут сохраняться снимки.
Внимание! Не указывайте здесь корневую папку (вида C:\, D:\ и пр.)
Опция существует главным образом для обратной совместимости с версиями 3.xx комплекса.
Иногда бывает полезным просматривать снимки экранов пользователей не через отчеты БОСС-Оффлайн, а напрямую из серверной папки с разбивкой по пользователям. В этом случае нужно включить данную опцию и при этом включение теневого копирования необязательно, т.к. теневое копирование необходимо для просмотров скриншотов через отчеты.
Также для данной опции необходимо в клиентских настройках разрешить данное сохранение на вкладке "Мониторинг: Снимки экранов".

Примечание: Если для организации настроена иерархия, то к пути в папке будет добавлена соотв. часть иерархии.

Формат файла
Укажите, как будут группироваться сохраненные снимки: по имени машины, пользователя, дате и пр.
В этой строке вы должны указать относительный путь внутри серверной папки (см. пред. опцию), используя переменные вида %переменная%.
В конце этого пути должно быть имя файла с расширением .jpg
Допустимые переменные:
%COMPLOC% - домен, DNS-суффикс или рабочая группа, в которую входит компьютер
%COMPNAME% - имя компьютера
%USERDOMAIN% - домен пользователя (в сокращенном формате)
%USERNAME% - имя пользователя
%DATE% - дата снимка в формате гггг-мм-дд
%TIME% - время снимка в формате чч_мм_сс
Таким образом, можно как угодно группировать снимки для удобного просмотра из серверной папки.

Занимать на диске не более N-мегабайт
Укажите максимальный размер серверной папки со снимками.
Если указать 0, то папка очищаться не будет.

Макс. длина заголовка скриншота
Для экономии места в базе данных можно ограничить длину заголовка скриншота. Если указать 0, то ограничений не будет.

См. также вкладку клиентских настроек "Мониторинг: Снимки экранов"

6.2.2.4. Мониторинг - Веб-камеры

Наиболее важные опции на этой вкладке:

Сохранять снимки в папке
Укажите папку на сервере, куда будут сохраняться снимки.
Внимание! Не указывайте здесь корневую папку (вида C:\, D:\ и пр.)

Примечание: Если для организации настроена иерархия, то к пути в папке будет добавлена соотв. часть иерархии.

Формат файла
Укажите, как будут группироваться сохраненные снимки: по имени машины, дате и пр.
В этой строке вы должны указать относительный путь внутри серверной папки (см. пред. опцию), используя переменные вида %переменная%.
В конце этого пути должно быть имя файла с расширением .jpg
Допустимые переменные:
%COMPLOC% - домен, DNS-суффикс или рабочая группа, в которую входит компьютер
%COMPNAME% - имя компьютера
%DATE% - дата снимка в формате гггг-мм-дд
%TIME% - время снимка в формате чч_мм_сс
Таким образом, можно как угодно группировать снимки для удобного просмотра из серверной папки.

Занимать на диске не более N-мегабайт
Укажите максимальный размер серверной папки со снимками.
Если указать 0, то папка очищаться не будет.

См. также вкладку клиентских настроек "Мониторинг: Веб-камеры"

6.2.2.5. Мониторинг - Автопрослушка

Наиболее важные опции на этой вкладке:

Сохранять аудио в папке
Укажите папку на сервере, куда будут сохраняться аудиозаписи.
Внимание! Не указывайте здесь корневую папку (вида C:\, D:\ и пр.)

Примечание: Если для организации настроена иерархия, то к пути в папке будет добавлена соотв. часть иерархии.

Формат файла
Укажите, как будут группироваться сохраненные записи: по имени машины, дате и пр.
В этой строке вы должны указать относительный путь внутри серверной папки (см. пред. опцию), используя переменные вида %переменная%.
В конце этого пути должно быть имя файла с расширением .ogg
Допустимые переменные:
%COMPLOC% - домен, DNS-суффикс или рабочая группа, в которую входит компьютер
%COMPNAME% - имя компьютера
%DATE% - дата начала записи в формате гггг-мм-дд
%TIME% - время начала записи в формате чч_мм_сс
Таким образом, можно как угодно группировать файлы для удобного просмотра из серверной папки.

Занимать на диске не более N-мегабайт
Укажите максимальный размер серверной папки с записями.
Если указать 0, то папка очищаться не будет.

См. также вкладку клиентских настроек "Мониторинг: Автопрослушка"

6.2.2.6. Мониторинг - Теневое копирование

Наиболее важные опции на этой вкладке:

Папка для сохранения файлов
Укажите **локальную** папку на сервере для сохранения файлов (рекомендуется на диске C:).
Внимание! При использовании сетевых и shared-папок правильная работа не гарантируется!

Занимать на диске не более
Можно ограничить максимальный размер папки (в МБ). Если указать 0, то очистка папки производиться не будет.

См. также вкладку клиентских настроек "Мониторинг: Теневое копирование"

6.2.2.7. Мониторинг - Цифровые отпечатки

При использовании **цифровых отпечатков**, в случае, если содержимое некоторых или всех важных файлов может иногда меняться, или могут добавляться новые файлы, то вместо ручного добавления каждого файла на странице цифровых отпечатков можно здесь указать список папок/файлов, откуда сервер будет периодически (один раз в час) обновлять цифровые отпечатки файлов. При этом удаление отпечатков из базы не происходит, даже если оригинальный файл был удален!
В каждой новой строке данного списка можно указывать путь к папке, файлу (допускается использование масок). Пример:

```
c:\documents\*.doc
c:\other\
\\server\file\data.pdf
```

Внимание! Пути должны быть доступны относительно сервера!

6.2.2.8. Распознавание текста (OCR)

На этой странице нужно выбрать способ и установить параметры оптического распознавания текста (OCR), которое используется в DLP-анализе (например, при распознавании текста на скриншотах, которые пользователь делает по нажатии клавиши PrintScreen).

ABBYY Cloud OCR
На сайте необходимо зарегистрироваться и создать **Application**. Название созданного Application и пароль для него нужно вписать в соотв. поля настроек.
Для распознавания данным способом нужен доступ в интернет с серверной машины на сайт **http(s)://cloud.ocrsdk.com**

6.2.2.9. Генератор отчетов - Параметры

Генератор отчетов служит для автоматической генерации отчетов по расписанию без участия пользователя.

Наиболее важные опции на этой вкладке:

Время генерации
Выберите периодичность и время генерации отчетов.
Если указана периодичность ПН-ВС, ПН-ПТ или ПН-СБ, то отчеты будут генериться каждый день в пределах выбранного диапазона. Соответственно и временной интервал в отчете будет равен одному дню.
Если указана периодичность "каждый ПН", "каждый ВТ", и т.д., то отчеты будут генериться раз в неделю в выбранный день. Соответственно и временной интервал в отчете будет равен одной неделе.
Внимание! День генерации отчета в сам отчет не включается!
Файл отчета за неделю будет в несколько раз больше файла за один день!

Рабочий день
Укажите длительность рабочего дня в часах (это используется в отчетах некоторых типов). Можно указывать не только целые числа (например, 7.5)

Внимание! Каждый начальник сам включает или выключает генератор отчетов в своем **личном кабинете**.
Администратор базы данных может запретить или разрешить тому или иному начальнику использовать автоматическую генерацию отчетов **в настройках прав** начальников.

6.2.2.10. Генератор отчетов - Отчеты (начальникам)

Существует возможность автоматической генерации отчетов для начальника по всем его подчиненным.

Выберите типы отчетов, которые вы хотели бы видеть в генерируемом общем отчете.
Чем больше выбрано отчетов, тем больше будет размер файла конечного общего отчета!
При этом, для каждого начальника администратором дополнительно устанавливаются разрешения на соотв. отчеты, потому в итоге отчет будет сгенерирован только если выбран на этой странице и разрешен для начальника в его правах!

Внимание! Каждый начальник сам включает или выключает генератор отчетов в своем **личном кабинете**.
Администратор базы данных может запретить или разрешить тому или иному начальнику использовать автоматическую генерацию отчетов **в настройках прав** начальников.

Таким образом, для включения такой генерации необходимо установить соотв. право начальнику (опция **"Разрешить автоматическую генерацию отчетов (для себя)"**), а также необходимо ему самому сделать настройки в своем **личном кабинете**.

6.2.2.11. Генератор отчетов - Отчеты (сотрудникам)

Существет возможность настроить отправку каждому сотруднику отчетов по самому себе.

Отчеты будут отправлены только тем сотрудникам, для которых в **досье** установлен **e-mail** (на этот же e-mail и будет отправляться отчет).
При этом опции e-mail-отправки должны быть также настроены на вкладке "Генератор отчетов: отправка на e-mail".

Для отправки отчетов сотрудникам необходимо настроить хотя бы одного начальника на автоматическую генерацию отчетов, при этом в правах для него дополнительно отметить опцию **"Разрешить автоматическую генерацию отчетов (для подчиненных)"**.

При этом, для каждого начальника администратором дополнительно устанавливаются разрешения на соотв. отчеты, потому в итоге отчет будет сгенерирован только если выбран на этой странице и разрешен для начальника в его правах!

Внимание! Каждый начальник сам включает или выключает генератор отчетов в своем **личном кабинете**.
Администратор базы данных может запретить или разрешить тому или иному начальнику использовать автоматическую генерацию отчетов **в настройках прав** начальников.

6.2.2.12. Генератор отчетов - Сохранение в папку

Наиболее важные опции на этой вкладке:

Сохранять отчеты в папке
Укажите папку на сервере, куда будут сохраняться отчеты.
Внимание! Не указывайте здесь корневую папку (вида C:\, D:\ и пр.)

6.2.2.13. Генератор отчетов - Отправка по FTP

Наиболее важные опции на этой вкладке:

Отправлять отчеты на FTP-сервер
Можно запретить или разрешить отправку отчетов на ваш FTP-сервер.

FTP-сервер
Укажите FTP-сервер для подключения (без префиксов типа ftp:// и пр.)

Порт
Укажите порт подключения (по умолчанию - 21).

Пользователь/Пароль
Укажите имя пользователя и его пароль на FTP-сервере. Именно под этим пользователем будет осуществлен вход на сервер.

Использовать анонимный доступ
Если ваш FTP-сервер позволяет использовать анонимный доступ и вы не хотите входить на FTP под конкретным пользователем, то можно использовать данную опцию.
Имя пользователя и пароль при этом игнорируются.

Использовать пассивный режим FTP
Режим работы определяет правила создания соединений для передачи данных по протоколу FTP. В обычном режиме по запросу программы FTP-сервер устанавливает TCP-соединение с вашей машиной, в пассивном соединение устанавливает сама программа. Обычный режим может не работать если в сети используется NAT, Firewall, либо другие технологии, ограничивающие прием входящих TCP-соединений. На некоторые FTP-сервера доступ в пассивном режиме ограничен.

Папка на FTP-сервере для сохранения отчетов
Укажите папку на FTP-сервере, куда будут сохраняться отчеты.
Внимание! Папка должна быть существующей!
Можно указывать путь относительно текущей папки (обычно она корневая) или относительно корневой (в этом случае нужно в начале пути указывать символ "/").
Если ничего не указать, то отчеты будут создаваться в текущей папке (обычно она корневая).
Если указать только символ "/", то всегда будут создаваться в корневой папке.
Не забывайте указывать символы "/" вместо "\" (как принято в системах Windows)!

Число попыток отправки при неудаче
Можно установить, сколько раз пытаться отправить отчет, если с первого раза по какой-то причине сделать этого не удалось.

6.2.2.14. Генератор отчетов - Отправка на e-mail

Наиболее важные опции на этой вкладке:

Отправлять отчеты на e-mail
Можно запретить или разрешить отправку отчетов на e-mail ящики начальников/сотрудников.

SMTP-сервер
Укажите SMTP-сервер для отправки писем. Можно использовать как сервер вашего интернет-провайдера, так и любой другой доступный. Если используется сервер провайдера, то настройки вы должны уточнить у него.
Можно использовать популярные бесплатные серверы smtp.mail.ru, smtp.yandex.ru, smtp.gmail.com (для последнего **отправка вложений может блокироваться**!)

Порт
Укажите порт подключения (по умолчанию - 587), может быть 25. Для SSL-соединений используйте порт 465.

Пользователь/Пароль
Укажите имя пользователя и пароль для SMTP-авторизации.
Обычно имя пользователя - это e-mail отправителя.
Если не требуется, то необходимо отметить галочку "Проверка подлинности не требуется".

Проверка подлинности не требуется
Если отметить, то имя пользователя и пароль игнорируются.

От кого
Укажите обратный e-mail отправителя. Должен присутствовать **обязательно**.
Причем, во избежание проблем, он должен быть **в том же домене, что и SMTP-сервер**! К примеру, при отправке через smtp.gmail.com должен быть вида имя@gmail.com, а также имя@gmail.com должно быть именем пользователя в данном случае.

Не отправлять письма большие чем N-мегабайт
Укажите здесь максимальный размер отправляемых писем.

Число попыток отправки при неудаче
Можно установить, сколько раз пытаться отправить отчет, если с первого раза по какой-то причине сделать этого не удалось.

Пример настроек:

```
SMTP-сервер: smtp.mail.ru
Порт: 587
Пользователь: ivanov@mail.ru
Пароль: ******
От кого: ivanov@mail.ru
```

6.2.2.15. Генератор отчетов - Отправка на веб-сайт

Существует возможность отправлять отчеты на ваш веб-сайт.
Данное действие аналогично тому, что вы на своем сайте разместите кнопку "Отправить файл" и будете передавать на веб-сервер файлы отчетов.
Далее вы можете их отправлять по почте, сохранять в папку на сервере или записывать в SQL-базу.
Обычно на стороне сервера файлы принимает php или cgi-скрипт.
На стороне клиента данные передаются через HTML-форму.
В параметре "Полный URL http POST-запроса" необходимо указать местоположение скрипта, выполняющего загрузку на сервер.
Следует также знать, что файл будет передан в переменной с именем **"uploadedfile"**. Именно это имя нужно использовать в скрипте на сервере.

Ниже приведены примеры файла клиента (HTML-страница) и скрипта на сервере (PHP), чтобы был более понятен функционал данной возможности:

```
; --------------------
; файл upload.html
; --------------------
<form enctype="multipart/form-data" action="http://mysite.com/action.php" method="POST">
<input name="uploadedfile" type="file"><br>
<input type="submit" value="Отправить файл">
</form>

; --------------------
; файл action.php
; --------------------
<?
// данная папка должна существовать на сервере!
$target_path = "uploads/";
$target_path = $target_path . basename($_FILES['uploadedfile']['name']);
if(move_uploaded_file($_FILES['uploadedfile']['tmp_name'], $target_path)) {
    echo "The file ".  basename( $_FILES['uploadedfile']['name']).
    " has been uploaded";
} else{
    echo "There was an error uploading the file, please try again!";
}
?>
```

Таким образом, функционал файла upload.html реализован в программе, что позволяет отправлять файлы автоматически!
А файл, подобный action.php, должен быть размещен у вас на веб-сервере.

6.2.2.16. Генератор отчетов - Отправка в файлообменник

Существует возможность отправлять отчеты в облачные файлообменники.
Настройка личных параметров входа в файлообменник осуществляется в **личном кабинете** каждого начальника.

6.2.2.17. Генератор отчетов - Угрозы

На этой странице есть возможность включить автоматический поиск угроз при генерации отчетов (в генераторе отчетов) или же при ручной генерации мастера отчетов в программе БОСС.
Сами же угрозы представляют собой отдельные слова (не фразы!), поиск которых будет осуществляться во всех сгенерированных отчетах (независимо от типа отчета).
Написание каждой новой угрозы должно начинаться с новой строки!
При этом если перед словом указать символ **тильды "~"**, то будет использоваться алгоритм **неточного сравнения слов**, учитывающий возможные опечатки и особенности языка.

6.2.2.18. Генератор уведомлений - Отправка на e-mail

Опции соответствуют настройкам страницы "Генератор отчетов: Отправка на e-mail".

6.2.2.19. Генератор уведомлений - Отправка по SMS

Настраивается возможность отправки уведомлений о событиях по SMS на мобильные телефоны начальников.
При этом начальник в своем **личном кабинете** должен разрешить такую отправку и указать свой номер телефона.
В строке запуска указывается путь к внешней программе с двумя обязательными параметрами:
%PHONE% - передается моб. тел. для отправки на него SMS;
%MESSAGE% - передается текст SMS-сообщения (UTF8 URL-encoded).
Программа должна выполнить отправку и завершить свою работу.
Сама отправка может идти любым способом, например через общедоступные платные SMS-шлюзы посредством всевозможных http-запросов, или же через стандартный USB GSM-модем (GPRS/3G/4G).
На странице загрузки комплекса (здесь) разработаны утилиты для отправки SMS. Более подробное описание утилит находится в справках к ним.

6.2.2.20. Генератор уведомлений - Интеграция с Telegram

Существует возможность отправки уведомлений о событиях в мессенджер Telegram на смартфоны начальников, а также отправка команд серверу от начальников через мессенджер.

Сначала администратору необходимо создать для организации своего Telegram-бота.
Для этого администратору нужно в своем мессенджере добавить в чат бота с именем **@botfather** и отправить ему сообщение **/newbot**, после чего ввести уникальное название и уникальное имя (username) вашего бота (username должно заканчиваться на "bot").
Пример:
Название: MyCompanyNotifier
Username: MyCompany_bot

После чего **@botfather** создаст вам бота и пришлет HTTP API token в чат. Скопируйте его в поле настроек на этой странице.
Пример токена: 123456:ABC-DEF1234ghIkl-zyx57W2v1u123ew11

1) Для получения уведомлений о событиях начальники самостоятельно в **личном кабинете web-интерфейса комплекса** должны включить опцию отправки уведомлений и получить там **chat_id**.

2) Для отправки команд серверу необходимо разрешить начальнику команды Telegram здесь, после чего начальник самостоятельно в **личном кабинете web-интерфейса комплекса** должен получить **chat_id**.
При желании сами команды можно изменить на этой странице в соответствующих полях.
Внимание! Команды блокировки и выключения применяются ко всем машинам, которые в данный момент подключены к серверу! Дополнительных предупреждений бот не выдает!

Внимание! Данные передаются на сервер **api.telegram.org:443** по защищенному https-протоколу через сервер комплекса, поэтому необходим доступ в Интернет к этому серверу Telegram на серверной машине (где установлен сервер комплекса)!
Также доступ к этому серверу необходим единоразово на машинах начальников при первоначальной регистрации подписки в личном кабинете.

Внимание! После изменения данных настроек, настроек прав для пользователей базы, настроек в личном кабинете, серверу необходимо около 1 минуты для применения настроек в силу!

6.2.2.21. Защита клиента

При включении данной опции сервер комплекса будет периодически проверять подключение клиентских машин, а также стандартный ping до клиентских машин. На основании полученной информации можно сделать вывод о возможном несанкционированном отключении клиентской части комплекса на машинах. Если такое произошло, то будет сделана запись в отчете "События: Компьютер", а также опционально сгенерировано уведомление начальникам для БОСС-Онлайн (настраивается на вкладке "События").
Событие будет сгенерировано не сразу, а спустя минимум 6-10 минут!
Событие будет генерироваться периодически примерно два раза в сутки (пока клиент не будет восстановлен).
Внимание! Данная функция не будет работать в ситуации когда команду ping нельзя выполнить по имени клиентской машины с серверной (обычно когда клиент и сервер находятся в разных сетях).

6.2.2.22. События

Здесь можно выбрать события, для которых будут отправляться мгновенные уведомления начальникам (через БОСС-Онлайн, SMS, e-mail).
Внимание! E-mail/SMS отправляются только для высокоприоритетных событий!

6.2.3. Клиентские настройки (компьютера):

6.2.3.1. Общие настройки

Наиболее важные опции на этой вкладке:

Никогда не переходить в отложенный режим работы
См. **Отложенный мониторинг**

Выполнять периодическую синхронизацию времени клиентов с серверным
При включении время на клиентских машинах будет периодически синхронизироваться с серверным. Т.е. будет таким, как на серверной машине.
Рекомендуется во избежание фальсификации данных в отчетах!

Дни недели и временные интервалы наблюдения
Вы можете отметить дни недели, в которые будет производиться наблюдение за клиентскими компьютерами. В другие дни наблюдение выполняться не будет.
Также можно указать временные интервалы, внутри которых будет выполняться наблюдение. Вне этих интервалов наблюдение выполняться не будет.
Сами временные интервалы задаются через запятую или точку с запятой в форматах: "чч:мм", "чч:м", "ч:мм", "ч:м", или "ч".
Допустимые значения для минут: 0-59, для часов: 0-23.
Допускается переход через 0:00, т.е. начало интервала может быть больше конца в абсолютном значении.
Пустая строка означает, что интервалов нет и наблюдение выполняться не будет вообще.
Интервал 0:00-23:59 означает, что наблюдение будет выполняться круглосуточно.
Пример интервала: 8:00-13:00,14:00-17:00

Выполнять автоматическое обновление при наличии в базе новой версии
Аналогично выполнению функции БОСС-Онлайн "Обновить клиентское ПО", но только в автоматическом режиме. См. раздел справки "Обновление комплекса" для более подробной информации.
Т.е. если в базу внесена новая версия после обновления администраторской части, то в течение 1-2 часов после этого произойдет загрузка данной версии на клиентскую машину. Активация новой версии клиента происходит только **после перезагрузки** клиентской машины!
Посмотреть текущую версию клиентской части можно через функцию БОСС-Онлайн **"Общие сведения"**.

Выполнять автоматическое удаление клиента
Данная опция служит для синхронизации с доменом. Например, в соотв. группах безопасности домена администраторы AD удалили клиентскую машину из списка наблюдаемых, - в этом случае при включении данной опции после проведения синхронизации с AD (в ручном или автоматическом режиме) клиент также будет удален с машины спустя некоторое время (от нескольких минут до нескольких часов).
Если же синхронизация с AD ни разу не проводилась, то данная опция не будет иметь эффекта.
Также опция не будет иметь эффекта если клиентский компьютер не входит в домен.

Ключ для удаления из командной строки
Если предполагается удалять клиентов через командную строку (например, в MS System Center), то необходимо для защиты установить здесь ключ (слово-пароль из английских букв и/или цифр без пробелов). См. также здесь.

Установить новое выводимое имя/описание клиентской службы
Если строки не пустые, то можно изменить имя/описание клиентской службы.
Примечание: изменения вступят в силу после перезагрузки клиентских машин.
Внимание! Администратор домена может скрыть клиентскую службу (см. здесь).

Настройки http-proxy
Некоторые функции (например, распознавание голоса) могут требовать выход в интернет по http-протоколу с клиентских машин (это обязательно оговорено в справке к каждой такой функции!). И если в вашей организации требуется обязательное использование http-proxy, то здесь можно установить необходимые настройки.

6.2.3.2. Мониторинг - Машинное время

Вы можете включить или отключить наблюдение за общим временем работы компьютера.
Если отключить, то эти данные в базу передаваться не будут.

6.2.3.3. Мониторинг - Веб-камеры

Наиболее важные опции на этой вкладке:

Получать и передавать на сервер снимки с веб-камер
Если отключить, то на сервер не будут передаваться снимки с веб-камер.
Это позволит сэкономить сетевой трафик.
Поддерживается не более 4-х веб-камер на одном компьютере.
Важно! При включении данной функции веб-камера не сможет использоваться другими приложениями!

Делать снимки каждые N-секунд
Не указывайте слишком маленькое значение, чтобы не нагружать сеть и не занимать много места файлами снимков.

См. также вкладку серверных настроек "Мониторинг: Веб-камеры"

6.2.3.4. Мониторинг - Автопрослушка

Наиболее важные опции на этой вкладке:

Вести постоянную аудиозапись с микрофонов
Если включить, то на сервер будет передаваться аудиозапись с микрофонов клиентских машин.

Новый файл каждые N-минут
Позволяет разбивать файлы для более удобного анализа (от 1 до 60 минут).

См. также вкладку серверных настроек "Мониторинг: Автопрослушка"

Разрешить преобразование речи в текст для БОСС-Онлайн
Внимание! Включая данную опцию вы автоматически соглашаетесь с тем, что голосовые переговоры сотрудников (в момент соотв. запроса из БОСС-Онлайн) будут передаваться в реальном времени на внешние серверы компании Google (по http/https протоколу) для анализа и преобразования.
Вы должны ознакомиться и принять политику конфиденциальности Google: http://www.google.ru/policies/privacy/
Также включив данную опцию вы соглашаетесь использовать ее только в не противоречащих закону случаях, как это указано в лицензионном соглашении к продукту (при его установке).
Примечание: исходящий трафик на машине сотрудника при этом преобразовании будет составлять примерно 0.17 Mb/s.
Внимание! Если в вашей организации необходимо использовать **proxy** для выхода в интернет с клиентских машин, то сделать необходимые настройки нужно на вкладке **"Общие настройки" для компьютера**!

6.2.3.5. Мониторинг - Контроль оборудования

Вы можете включить или отключить передачу данных об оборудовании компьютера на сервер.
Если отключить, то эти данные в базу передаваться не будут.

6.2.3.6. Мониторинг - Чаты-звонки

Наиболее важные опции на этой вкладке:

Перехват сообщений чата Битрикс24
Если опция включена, то будет осуществлен перехват сообщений чатов Битрикс24 в десктоп-приложении и на сайте. При использовании облачной версии Битрикс24 поле сервера нужно оставить пустым, а при использовании корпоративного сервера Битрикс24 нужно указать его имя без префиксов https://, http://. Если используется нестандартный порт, то его нужно указать через двоеточие после имени сервера, а также добавить на странице Сетевой драйвер.
Внимание! Для работы опции должен быть включен Сетевой драйвер
Внимание! После включения опции ее активация произойдет при следующем запуске клиента Битрикс, или перезапуска сайта Битрикс на клиенте!

См. также вкладку настроек "Мониторинг: Чаты/звонки" для пользователя.

6.2.3.7. Сетевой драйвер

Сетевой драйвер используется для перехвата и контроля сетевого трафика на низком уровне.
При отключении не будет перехвата сетевых данных.
По умолчанию (неявно) для перехвата добавлены процессы популярных браузеров, почтовых клиентов, Skype, а также стандартные порты поддерживаемых протоколов (SMTP,POP3,HTTP(S),FTP). Можно добавить нестандартные TCP-порты для мониторинга (например, при использовании прокси), а также исключить некоторые порты. Аналогично и с процессами, для которых проводится мониторинг. Все данные нужно указывать через запятую списком.

В отличие от программ (процессов), запущенных пользователем, сетевой драйвер перехватывает трафик от всех служб (что сделано главным образом для поддержки перехвата трафика при использовании некоторых антивирусов), однако бывают ситуации, когда некоторые службы нужно добавить в исключения и не вести перехват. В **исключения для служб** нужно добавлять exe-файлы служб (не имена служб!), а также допускаются маски. Например, *.* запретит полностью мониторинг трафика от всех служб.

Опцию блокирования протокола QUIC рекомендуется использовать для корректного перехвата данных в Google-сервисах.

Важно отметить, что для перехвата зашифрованного (SSL) трафика используется установка в систему корневого сертификата с названием **"Local NetFlt CA 2"**. При этом, некоторые программы используют свою базу корневых сертификатов, поэтому могут выдавать предупреждение.
Например, браузер Яндекс (процесс browser.exe) выдает предупреждение в любом случае.
Для большинства браузеров и почтовых клиентов предупреждений не будет если клиент был установлен когда окна этих приложений были закрыты. В противном случае нужно перезагрузить клиентскую машину, или выполнить завершение сеанса, или же добавить сертификат в доверенные в самом приложении в окне предупреждения.

В **исключениях** можно добавить IP-адреса или имена хостов, для которых не будет использоваться сетевой драйвер. Обычно это бывает нужно делать для сайтов, которые чувствительны к подмене SSL-сертификата.
Каждое исключение в списке должно начинаться с новой строки.
Можно указывать DNS-имя (допускаются маски "*" и "?"), точный IP-адрес (IPv4/IPv6), IP-адрес с масками, а также диапазоны адресов (только IPv4).
Примеры:
134.17.23.*
192.168.1.15-192.168.1.20
10.10.1.5
*.dep.domain.com

Важно отметить, что для перехвата посещаемых URL в браузерах для отчетов сетевой драйвер не используется!

В старых ОС - Windows XP и Windows 7 (без выполненного Windows Update) драйвер работать не будет!

Внимание при использовании антивирусов! Очень редко бывает конфликтная ситуация, когда сразу после установки клиента блокируется сетевой трафик, в этом случае нужно выполнить перезагрузку. Если же используется удаленная установка на группу машин, то можно предварительно включить опцию **"Активировать драйвер только после перезагрузки"**, в этом случае конфликт будет исключен, но перехват начнет работать только после перезагрузки клиентских машин!

6.2.3.8. Выборочное наблюдение

Наиболее важные опции на этой вкладке:

Вести наблюдение "только за этими" или "за всеми, кроме этих" пользователей компьютера(ов)
Включая опцию вы можете указать пользователей компьютера, за которыми будет (или не будет) производиться наблюдение.
Данная опция обычно используется для **терминальных серверов**.
Для указания имени пользователя можно использовать **маски "*" и "?"**.
Допустимо указывать имена пользователей в форматах **пользователь** и **домен\пользователь** (при этом **домен указывать в сокращенном формате** - без точек!).
Если опцию не включать, то будет производиться наблюдение **за всеми** пользователями компьютера(ов).

Применять данное ограничение только на машинах с ОС Windows Server
Если опция выборочного наблюдения включена, то включение данной опции означает, что за рабочими станциями будет вестись наблюдение в обычном режиме (все пользователи), а вот к серверным машинам (обычно терминальным серверам) будет применено ограничение.
Использование данной опции полезно, когда нужно ограничить набор наблюдаемых пользователей терминального сервера, но не ограничивать никак на обычных рабочих станциях.

Внимание! Требуется выход (LogOff) пользователей для применения данных настроек, если настройки затрагивают этих пользователей!

6.2.3.9. Локальное хранилище

На этой странице есть возможность настроить локальное хранилище, т.е. локальную базу данных на компьютере клиента, которая используется когда нет связи с сервером и в режиме **отложенного мониторинга**. В таких случаях все данные наблюдений накапливаются в данной базе до возобновления связи или выхода из режима отложенного мониторинга соотв.

Наиболее важные опции на этой вкладке:

Время хранения, макс. объем базы и трафик
Не указывайте слишком большие значения, т.к. во-первых, будет больше использоваться места на диске клиентского компьютера (главным образом из-за файлов теневого копирования), а во-вторых, при передаче данных может быть увеличена нагрузка на сервер и его базу данных!

Не выполнять, если свободного места менее
Если на диске C: клиентской машины свободного места менее указанного числа МБ, то сохранения в локальном хранилище не будет и данные пропадут.

6.2.3.10. Запреты

Наиболее важные опции на этой вкладке:

Запретить запись на съемные (Flash) накопители
При включении пользователи не смогут записывать/сохранять/копировать данные на flash-диски.

Запретить FTP-протокол
Запрещает прием и передачу файлов через FTP/FTPS/SFTP
Необходимо, чтобы был включен Сетевой драйвер

Запретить доступ к web-сайтам
Можно указать списком (каждый сайт с новой строки) DNS-имена (не URL!) веб-сайтов, доступ к которым будет блокироваться через стандартные веб-браузеры. Допускается использование масок.
Необходимо, чтобы был включен Сетевой драйвер

См. также вкладку настроек пользователя "Запреты"

6.2.3.11. События

Здесь выбираются события, которые будут передаваться на сервер для записи в отчет "События".
Для настройки мгновенных уведомлений см. вкладку настроек **сервера** "События".

6.2.4. Клиентские настройки (пользователя):

6.2.4.1. Общие настройки

Наиболее важные опции на этой вкладке:

Никогда не переходить в отложенный режим работы
См. **Отложенный мониторинг**

Тип наблюдения
При наблюдении с уведомлением пользователю будет выдаваться сообщение в системном трее каждый раз при старте системы. Сам текст сообщения вы можете изменять.
При наблюдении без уведомления никаких уведомлений выдано не будет.

Дни недели и временные интервалы наблюдения
Вы можете отметить дни недели, в которые будет производиться наблюдение за клиентскими пользователями компьютера. В другие дни наблюдение выполняться не будет.
Также можно указать временные интервалы, внутри которых будет выполняться наблюдение. Вне этих интервалов наблюдение выполняться не будет.
Сами временные интервалы задаются через запятую или точку с запятой в форматах: "чч:мм", "чч:м", "ч:мм", "ч:м", или "ч".
Допустимые значения для минут: 0-59, для часов: 0-23.
Допускается переход через 0:00, т.е. начало интервала может быть больше конца в абсолютном значении.
Пустая строка означает, что интервалов нет и наблюдение выполняться не будет вообще.
Интервал 0:00-23:59 означает, что наблюдение будет выполняться круглосуточно.
Пример интервала: 8:00-13:00,14:00-17:00

6.2.4.2. Мониторинг - Пользовательское время

Вы можете включить или отключить наблюдение за временем работы пользователя (его входом/выходом в/из системы). Если отключить, то эти данные в базу передаваться не будут.
Опция особенно актуальна для терминальных сессий. С ее помощью можно контролировать время начала и конца работы пользователя по дням, т.к. опция мониторинга **машинного** времени будет малоинформативна для терминального сервера.
Также при отключенной опции не будет видна общая активность пользователя в отчетах.

6.2.4.3. Мониторинг - Программы-сайты

Наиболее важные опции на этой вкладке:

Вести мониторинг запускаемых приложений и сайтов
Если отключить, то в базу не будут передаваться сведения о запущенных пользователем программах/сайтах и не будет передаваться вводимый пользователем текст.

Список корпоративных сайтов
Можно указать список сайтов, которые не будут попадать в отчет "Сайты", а будут идти в отчет "Программы".
Обычно это бывает нужно, если в компании сотрудниками часто используются корпоративные сайты почты или другие и нет особого смысла рассматривать эти сайты как внешние ресурсы развлекательного и пр. характера.
Каждый сайт нужно указывать с новой строки! Можно указывать как полный, так и частичный URL.
Примеры:
http://corp.mail/mail
1c.ourcorp.ru
Внимание! При внесении изменений в список корпоративных сайтов, данные об активном времени работы в отчетах "Сводный" и "Программы/Сайты" могут отличаться в текущий день изменения настроек. Совпадать начнут только со след. дня!

Передавать в базу иконки приложений
Если отключить, то в базу не будут передаваться иконки приложений. Также их не будет видно и в отчетах. Это слегка помогает сэкономить сетевой трафик.

Не передавать в программу "БОСС-Онлайн" заголовок текущего окна
Также слегка помогает сэкономить сетевой трафик.

Разрешить мониторинг TeamViewer-сессий и подобных программ
Если отключить, то активность и вводимый текст в удаленных TeamViewer-сессиях фиксироваться не будут.
При включенной опции под мониторинг могут попасть и действия программ, которые имитируют клики и нажатия клавиш.
Данная опция не влияет на сессии RemoteDesktop!

6.2.4.4. Мониторинг - Вводимый текст

Наиболее важные опции на этой вкладке:

Вести мониторинг вводимого текста с клавиатуры
Если отключить, то в базу не будет передаваться вводимый пользователем текст.

Передавать в базу вводимые пароли в программах
Внимание! Мы не можем гарантировать, что при отключении данной опции со всех программ перестанут собираться пароли! Данный функционал очень специфичен для каждой программы индивидуально.

6.2.4.5. Мониторинг - Буфер обмена

Наиболее важные опции на этой вкладке:

Вести мониторинг текста/изображений в буфере обмена
Если отключить, то в базу не будет передаваться текстовое содержимое и картинки из буфера обмена пользователя. Мониторинг файлов в буфере обмена настраивается на вкладке "Файловые операции".
Для перехвата изображений необходимо включить опцию "Теневое копирование" в клиентских и серверных настройках!

Запретить буфер обмена при активном сеансе Remote Desktop
Можно включить данную опцию, чтобы при работе с удаленным сервером через программу Remote Desktop пользователи не смогли копировать с сервера изображения/текст через буфер обмена на свой локальный компьютер. При этом, чтобы внутри самой удаленной сессии буфер обмена работал в обычном режиме, нужно отключить опцию использования буфера обмена при подключении к удаленному серверу в настройках программы Remote Desktop.

6.2.4.6. Мониторинг - Снимки экранов

Наиболее важные опции на этой вкладке:

Получать и передавать на сервер снимки с экранов
Если отключить, то на сервер не будут передаваться экраны пользователей. Это позволит сэкономить сетевой трафик.

Делать снимки каждые N-минут
Не указывайте слишком маленькое значение, чтобы не нагружать сеть и не занимать много места файлами снимков.

Сохранять снимки только в отчете БОСС-Оффлайн
Снимки можно будет просматривать только в отчете "Снимки экранов" БОСС-Оффлайн. При этом необходимо **включение теневого копирования на клиенте и сервере!**

Сохранять снимки только в папке на сервере
Иногда бывает полезным просматривать снимки экранов пользователей не через отчеты БОСС-Оффлайн, а напрямую из серверной папки с разбивкой по пользователям. В этом случае нужно включить данную опцию и при этом включение теневого копирования необязательно, т.к. теневое копирование необходимо для просмотров скриншотов через отчеты. Также при этом необходимо будет в серверных настройках настроить папку и опции сохранения на вкладке "Мониторинг: Снимки экранов".

Сохранять снимки в отчете и папке одновременно
Объединение вышеописанных опций.

Опции снимков
Ряд опций, позволяющих настроить сохранение снимков.
С их помощью можно снизить нагрузку на сетевой трафик и уменьшить занимаемое снимками место ценой качества изображения. Потому необходимо подобрать параметры исходя из ваших требований.

6.2.4.7. Мониторинг - Снимки экранов (доп.)

Можно выбрать, для каких приложений или сайтов будут сниматься специальные скриншоты "по изменению контента", чтобы не пропустить важный текст или другую информацию в окне.

"Интервал проверки содержимого окна" определяет, как часто будет контент окна сверяться с предыдущим, т.е. фактически определяет максимальную частоту съема скриншотов.

"Минимальное кол-во отличающихся пикселей" используется при сравнении текущего и предыдущего содержимого окна (по-пиксельно). Если разница в пикселях превышает данное значение, то снимок окна будет сделан.

В правилах для приложений/сайтов можно использовать:

1) Переменные:
@exe@ - exe-файл приложения без пути;
@class@ - класс окна (для определения класса можно использовать утилиту);
@url@ - полный URL сайта;
@title@ - заголовок окна.

2) Логические операторы: **OR** (или), **AND** (и)

3) Скобки **(** и **)**.

4) Операторы сравнения: **=** (равно), **!=** (не равно), **LIKE** (сравнение по маске).
В качестве масок можно использовать: **%** (ни одного, один или несколько символов) и **_** (один символ).

Внимание! При сравнении строк операторы **=**, **!=** чувствительны к регистру и если эта чувствительность не нужна (например, при сравнении имен файлов), то нужно использовать сравнение **LIKE**.
Внимание! Строки в правилах необходимо указывать в **одинарных кавычках**!

Таким образом можно организовать гибкую проверку условий для того или иного приложения/сайта.

Пример 1: необходимо создать правило для приложения с exe-файлом "app.exe", классом окна "WndClass_0" и чтобы заголовок окна включал слова "Workbench" или "Setup":

```
(@exe@ LIKE 'app.exe') AND (@class@='WndClass_0') AND ((@title@ LIKE '%Workbench%') OR (@title@ LIKE '%Setup%'))
```

Пример 2: необходимо создать правило для сайта "https://work.company.com":

```
@url@ LIKE 'https://work.company.com%'
```

6.2.4.8. Мониторинг - Печать на принтере

Наиболее важные опции на этой вкладке:

Вести мониторинг печатаемых на принтере документов
Если отключить, то в базу не будет передаваться информация о распечатанных пользователями документах.

Мониторинг в контексте пользователя
Для мониторинга **сетевых** принтеров нужны администраторские права. Потому, если пользователь не имеет таких прав и является ограниченным, мониторинг для него не будет возможен. В этом случае необходимо указать, что мониторинг будет выполнен в контексте другого пользователя-администратора. Необходимо указать домен этого администратора (если есть), его имя и пароль (с пустыми паролями работать не будет!).
Например, если на всех клиентских машинах есть администраторский пользователь под именем "Administrator", то нужно убедиться, что его пароль не пустой и он везде одинаков, после чего вписать его в эту опцию.
Не стоит путать этого пользователя с пользователем на сервере! Данный вводимый пользователь может быть либо членом домена, либо находиться на локальных клиентских машинах.
Если же пользователь и так работает с администраторскими правами, то в данной опции ничего указывать не нужно!

Внимание! При использовании Shared (общих) принтеров:
Для мониторинга shared-принтеров необходимо использовать специальную утилиту (загружается здесь), которую необходимо установить на принт-сервер(ы), к которым подключены принтеры. В этом случае опцию "Вести мониторинг печатаемых на принтере документов" можно отключить (если все принтеры общие).
В **терминальных** сессиях необходимо в настройках доступа принтера указать конкретных пользователей, а не оставлять **"Everyone"**!

Внимание! Для **перехвата файлов** принтера необходимо включить опцию "Теневое копирование" в **клиентских и серверных** настройках!
Файлы принтера представлены не в оригинале, а в виде файлов спулера (.spl/.shd). Для их просмотра необходимо использовать сторонние утилиты.
Можно найти по поиску в интернете "SPL Viewer".
Примеры утилит:
http://www.lvbprint.de/html/splviewer1.html
http://www.prnwatch.com/pviewer.html
Также существует возможность **повторной отправки файлов спулера на принтер** для анализа оригинальных документов уже на бумажном носителе. Для этого используйте бесплатную утилиту **PrintSPL**, которую можно скачать здесь.

Внимание! Данные настройки вступают в силу только после перезагрузки клиентской машины!

6.2.4.9. Мониторинг - Файловые операции

Вы можете включить или отключить наблюдение за различными файловыми операциями на разных типах носителей.
Под файловыми операциями понимаются: копирование, перенос, удаление и копирование в буфер обмена.
Имеется возможность также наблюдать за выбранными папками. В этом случае необходимо указать список таких папок, используя в качестве разделителя точку с запятой (можно использовать и переменные окружения %переменная%).
К **теневому копированию** чувствительны все копирования на сменные носители, а также копирования в **выбранные папки**. См. также настройки **"Теневое копирование"**.

6.2.4.10. Мониторинг - Отправка файлов

На этой странице настраивается возможность мониторинга отправки файлов через сайты-файлообменники (depositfiles.com, files.mail.ru и пр.), отправки вложений писем через сайты почтовых систем (mail.ru, gmail.com и пр.), а также почтовые программы (Outlook, Mail, Bat, LotusNotes, Thunderbird) и чаты Skype, Telegram, WhatsApp, Trillian, Viber, ICQ, Mail.ru Agent, QIP, Lync.

6.2.4.11. Мониторинг - Почта

На этой странице настраивается возможность перехвата входящих и исходящих писем в почтовых клиентах. Необходимо, чтобы был включен Сетевой драйвер

Внимание! Для перехвата писем необходимо включить опцию "Теневое копирование" в клиентских и серверных настройках!

6.2.4.12. Мониторинг - Чаты-звонки

На этой странице настраивается возможность перехвата входящих и исходящих сообщений в программах-чатах (например, QIP/ICQ/Skype/Lync/Viber), а также звонков в Skype/Lync/Viber.

Наиболее важные опции на этой вкладке:

Порты
Если используются нестандартные порты, то можно их добавить через запятую.

Перехватывать и сохранять голосовые переговоры
При включении будут передаваться на сервер в режиме теневого копирования аудио-файлы переговоров (просмотр в отчете "Чаты/звонки").
Внимание для Windows XP-клиентов! Будет осуществлен перехват только голоса сотрудника, но не его собеседника!
Внимание! Для перехвата голоса необходимо включить опцию "Теневое копирование" в клиентских и серверных настройках!

Преобразовывать голосовые переговоры в текст
Внимание! Включая данную опцию вы автоматически соглашаетесь с тем, что голосовые переговоры сотрудников в поддерживаемых перехватом программах будут передаваться в реальном времени на внешние серверы компании Google (по http/https протоколу) для анализа и преобразования.
Вы должны ознакомиться и принять политику конфиденциальности Google: http://www.google.ru/policies/privacy/
Также включив данную опцию вы соглашаетесь использовать ее только в не противоречащих закону случаях, как это указано в лицензионном соглашении к продукту (при его установке).
Примечание: исходящий трафик на машине сотрудника при этом преобразовании будет составлять примерно 0.17 Mb/s.
Внимание! Если в вашей организации необходимо использовать **proxy** для выхода в интернет с клиентских машин, то сделать необходимые настройки нужно на вкладке **"Общие настройки" для компьютера**!

6.2.4.13. Мониторинг - Теневое копирование

Наиболее важные опции на этой вкладке:

Передавать на сервер копии отправляемых/выводимых файлов пользователями и скриншоты
Существует возможность следить за содержимым отправляемых пользователем файлов в интернет, а также копируемых на сменные носители или выбранные пользователем папки на странице "Файловые операции" (нужно главным образом для того, чтобы предупредить утечку важной информации). В этом случае эти файлы или их части (если файлы большие) будут сохраняться на сервере и можно будет их просмотреть через отчеты **"Отправка файлов"** и **"Файловые операции"** (кликнув на соотв. ссылку).
Соответственно данная опция имеет смысл только если включен режим **мониторинга файловых операций и/или мониторинг отправляемых файлов**.
Также данная опция необходима для мониторинга **входящих/исходящих писем**, **снимков экранов**, **голосовых переговоров** и в будущем возможно и других отчетов.

Интересующие типы файлов
Укажите через запятую маски файлов, которые будут передаваться на сервер. Для всех файлов нужно указать *.*

Макс. размер файла или его части для сохранения
Если нужный файл меньше выбранного размера, то будет передан полностью, а иначе будет передана только его часть (первые N-байт) или же пустой файл (при включении опции **"Передавать пустые файлы, если размер превышен макс."**). Чем больше выбранный размер, тем больше нагрузка на сеть, потому не рекомендуется выбирать слишком большое число!
В текущей версии макс. размер можно выбрать **не более 32 МБ!**

Не выполнять, если свободного места менее N-мегабайт
Если на системном диске (обычно C:) компьютера пользователя менее указанного числа МБ свободного места, то теневое копирование выполняться не будет.

См. также вкладку серверных настроек "Мониторинг: Теневое копирование"

6.2.4.14. Мониторинг - Черный ящик

В этом режиме все действия пользователя (видео с экрана и звуки) будут сохраняться в локальные файлы на его машине в зашифрованном виде.

Путь к папке для сохранения
Данный путь может содержать переменные окружения для пользователя и компьютера (например, %USERPROFILE% - это "C:\Users\имя_пользователя\"). Можно использовать и сетевые пути, однако это крайне не рекомендуется из-за возможных проблем с производительностью!
Внимание! Не допускаются корневые пути вида C:\, D:\ и т.д.
В состоянии LogOff (завершенный сеанс) значение %USERPROFILE% это обычно "C:\Users\Default\".

Не выполнять, если свободного места менее
Если на диске, куда сохраняются файлы, менее N-мегабайт свободного места, то сохранения файлов не произойдет.

Время хранения записанных данных
Это ретроспектива хранения старых записей.

Ключ для шифрования файлов
Рекомендуется шифровать файлы и не оставлять это поле пустым (используется шифрование AES-256).
Каждый файл представляет собой запись длительностью в **один час** (формат - mp4) и при этом имеет нечитабельное имя и расширение **.dump**
Если файл зашифрован, то его невозможно открыть плеером и понять что это mp4-файл.
После расшифровки имя файла становится читабельным, расширение меняется на .mp4 и он становится открываемым для плееров.
Если ключ шифрования не использовался, то после расшифровки просто происходит преобразование имени файла в читабельное.
Для расшифровки необходимо использовать утилиту **mp4decrypt** с этим же ключем.
Внимание! При неправильном вводе ключа файл будет испорчен и не подлежит восстановлению!

Записывать видео с экрана
Запись видео идет с активного в данный момент монитора (на котором курсор мыши). Важным параметром при записи видео является **интервал между кадрами** - чем больше это значение, тем меньше файлы и меньше нагрузка на ресурсы клиентской машины, и наоборот. Минимальное значение - 1 сек, максимальное - 3600 сек.
Средний размер часового файла с настройками по умолчанию обычно **около 100 МБ**.

Записывать аудио с микрофона
Добавлять непрерывную запись с микрофона (используется микрофон по умолчанию в системе на клиентской машине).

Записывать аудио с динамиков
Добавлять непрерывную запись с динамиков компьютера.
Внимание! На некоторых звуковых картах иногда при включении этой опции может возникнуть ситуация "зацикливания" звуков после окончания воспроизведения некоторых или отсутствие звучания. Прекращается ситуация после след. воспроизведения любого звука. Если это часто имеет место быть, то лучше отключить данную опцию.

Внимание! Весь данный функционал "черного ящика" не будет работать, если в системе не установлен **Windows Media Foundation**. По умолчанию он не установлен на всех серверных ОС, а также на старых ОС Windows XP.

6.2.4.15. Мониторинг - Геолокация

Опцию передачи данных о местоположении компьютера имеет смысл включать для ноутбуков с Windows 8 и выше, которые могут менять свое местоположение.

Внимание! При включении на клиентских машинах может кратковременно появиться иконка геолокации в системном трее!

6.2.4.16. Мониторинг - Мобильный клиент

На этой странице настраиваются опции мониторинга для мобильного клиента.
Рекомендуется сразу изменить **пин-код администратора** для защиты от удаления клиента!

6.2.4.17. Запреты

Наиболее важные опции на этой вкладке:

Запретить использование Flash-накопителей
При включении пользователи не смогут работать с flash-дисками. Вместо этого будет выдано сообщение в трей о невозможности использования.

"Черный" и "белый" списки приложений
Можно указать списки приложений для запрета или разрешения соответственно.
Каждое приложение должно указываться с новой строки и представлять собой либо полный путь к исполняемому файлу, либо только сам exe-файл без пути, или описание приложения (название из его оригинального поля Description).
Допускается использование переменных окружения.
Примеры:

```
%WinDir%\Syswow64\regedit.exe
bad_app.exe
Microsoft Office Word
```

В случае попадания приложения под запрет запуска, будет выдано сообщение в трее на машине пользователя, и само приложение будет закрыто.
Важно отметить, что под контроль попадают только приложения **с окнами**, а скрытые системные приложения - нет!

См. также вкладку настроек компьютера "Запреты"

6.2.4.18. Угрозы

Здесь вы можете настроить угрозы, к которым будет чувствительна программа.
Каждая угроза должна быть написана с новой строки!
Угрозой может быть: **вход на сайт**, **запуск программы**, **ввод слова**.
Можно указывать:
- полный или частичный адрес сайта,
- заголовок сайта (или его часть),
- заголовок программы (или его часть),
- имя EXE-файла программы (если указывать путь, то только с переменными окружения вида %переменная%),
- описание программы (можно частичное),
- одиночное слово (не фразу!), при этом если перед словом указать символ **тильды "~"**, то будет использоваться алгоритм **неточного сравнения слов**, учитывающий возможные опечатки и особенности языка.
- шаблоны: **@CREDITCARD@** (ввод номера банковской карточки), **@PHONE@** (ввод номера телефона), **@EMAIL@** (ввод e-mail-адреса)

Реакция на угрозы настраивается на вкладке настроек **"События"**.

6.2.4.19. DLP в документах, картинках, голосе

На этой странице можно настроить **DLP (предотвращение утечек информации)** в документах/картинках/голосе.

Если пользователь будет совершать то или иное (выбранное в этих настройках) действие с определенными объектами, **в тексте которых** присутствуют одно или несколько совпадений из списка чувствительности, то будет сформировано событие, которое может быть далее записано в отчет "События" и выдано мгновенное уведомление в БОСС-Онлайн.
События настраиваются на вкладке **"События"**.
Также существует возможность запретить те или иные действия.

Если некоторые важные файлы компании меняются редко или не меняются совсем, то имеет смысл снять с них "цифровые отпечатки" и не вводить список чувствительности вручную. Более подробно см. "Цифровые отпечатки".

Правила заполнения блока "чувствительность":
- каждый новый элемент списка должен начинаться **с новой строки**;
- если необходимо точное совпадение, то можно указать одно слово или фразу без префиксов;
- если необходим **неточный поиск слов**, то можно указать одиночное слово (**не фразу!**) с префиксом "~";
- можно использовать шаблоны: **@CREDITCARD@** (номер банковской карточки), **@PHONE@** (номер телефона), **@EMAIL@** (e-mail-адрес).

Внимание! Для работы DLP необходимо чтобы **не были отключены** соотв. опции мониторинга на одноименных вкладках настроек (например, мониторинг буфера обмена, файловых операций и т.д.)

Внимание! Работа DLP ориентирована на вывод файлов, а не ввод, потому, к примеру, такое действие как копирование файлов из сменного носителя фиксироваться не будет!

Внимание! Следует отметить, что обойти можно любую DLP-защиту, потому система не может гарантировать защиту от утечек во всех возможных случаях, однако использование данной опции позволит в большинстве случаев если не предотвратить утечку, то дать возможность выявить нарушителя внутренних правил компании!

6.2.4.20. Нетипичное поведение

На этой вкладке настраивается возможность отслеживания нетипичного поведения сотрудника по ряду критериев. При возникновении такого поведения, в соответствии с настройками на вкладке **"События"** происходит генерация события.
Интервал отслеживания - задает время наблюдения, в течение которого ведется подсчет всех настраиваемых далее критериев.
Если в течение данного времени любой из критериев превысил указанное в настройках значение, то происходит событие.
Если указано значение **0**, то данный критерий не используется.
ShadowCopy файл - это файл, тип (расширение) которого соотв. настроенному на вкладке **"Теневое копирование"**.
"Выбранные папки" - папки, настраиваемые на вкладке **"Файловые операции"**.

Внимание! Для работы данной опции необходимо включение соотв. настроек на вкладках **"Теневое копирование"**, **"Файловые операции"**, **"Буфер обмена"**, **"Отправка файлов"**, **"Программы/сайты"**.

6.2.4.21. События

Здесь выбираются события, которые будут передаваться на сервер для записи в отчет "События".
Для настройки мгновенных уведомлений см. вкладку настроек **сервера** "События".

6.2.4.22. Аутсорсинг

На этой странице есть возможность разрешить сотруднику самому включать или выключать наблюдение за собой. Это бывает полезно при работе в режиме "аутсорсинга" на своем собственном компьютере.
При включении такого режима появляется иконка в трее, через которую можно включать или отключать наблюдение.

6.2.5. Группы

Группы пользователей и компьютеров нужно использовать, если вы **не хотите, чтобы клиентские настройки были одинаковыми для всех** компьютеров/пользователей и необходимо реализовать возможность установки своих индивидуальных настроек для определенных групп или отдельных пользователей/компьютеров.
В этом случае необходимо сопоставить такие группы с созданными профилями настроек. Для создания профилей настроек необходимо вывать **выпадающее меню** рядом с кнопками "Для компьютеров", "Для пользователей".

Пример: для определенных пользователей необходимо установить частоту съема скриншотов 1 раз в минуту, а для всех остальных - 1 раз в 10 минут.
В этом случае нажимаем кнопку настроек "Для пользователей" и обычным образом устанавливаем частоту скриншотов 1 раз в 10 минут.
Далее нажимаем в выпадающем меню рядом с кнопкой настроек "Для пользователей" - "Профиль №1" (как пример) и в настройках данного профиля устанавливаем частоту съема скриншотов 1 раз в минуту.
Далее нажимаем кнопку "Группы" и сопоставляем нужных пользователей с профилем №1.

Внимание! Для профилей сохраняются только лишь те настройки, которые вы изменяли в данном профиле. Остальные настройки берутся из базовых. К примеру, если в профиле №1 вы изменили только лишь частоту съема скриншотов, а потом в базовых настройках изменили размер файлов теневого копирования, то для профиля №1 размер файлов теневого копирования автоматически будет взят из базовых настроек, а не тот, который был на момент создания профиля!

Примечание: назначение профиля "пусто" означает использование базовых настроек (без профилей).

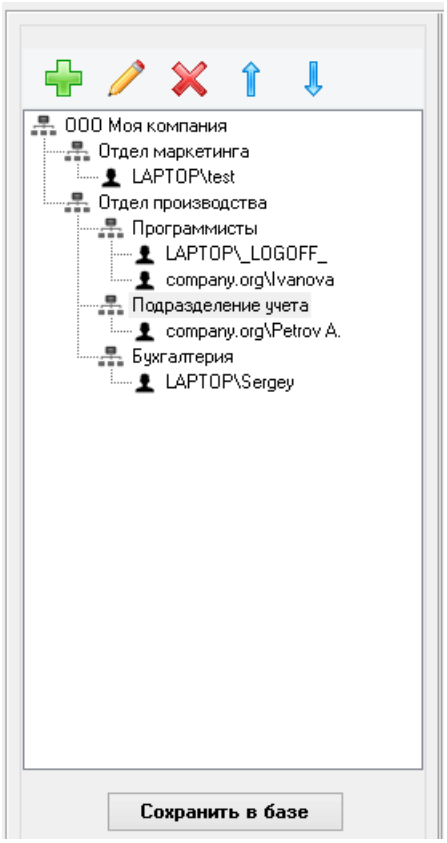
Примечание: списки пользователей и компьютеров в этом окне берутся из базы данных, а потому сразу после установки комплекса могут быть пустыми. Необходимо подождать 5-10 минут пока данные отчетов начнут поступать в базу от клиентских машин.

6.3. Структура компании

На этой странице можно опционально создать иерархическую структуру компании, с указанием отделов, подразделений и т.д.
В каждый отдел можно добавлять пользователей и компьютеры, которые еще не распределены по отделам. Сами списки пользователей/компьютеров (которые справа в колонках) будут доступны только после поступления первых данных наблюдения в базу (т.е. спустя 5-10 мин. после первой установки клиентских частей на машины пользователей).
Причем, нет необходимости распределять всех. Каждый пользователь или компьютер может быть либо в иерархии, либо нераспределенным в списке, но не может быть одновременно и там, и там!
Иерархия используется при отображении в БОСС-Онлайн, БОСС-Оффлайн и очень удобна для задания прав доступа начальникам к своим отделам.

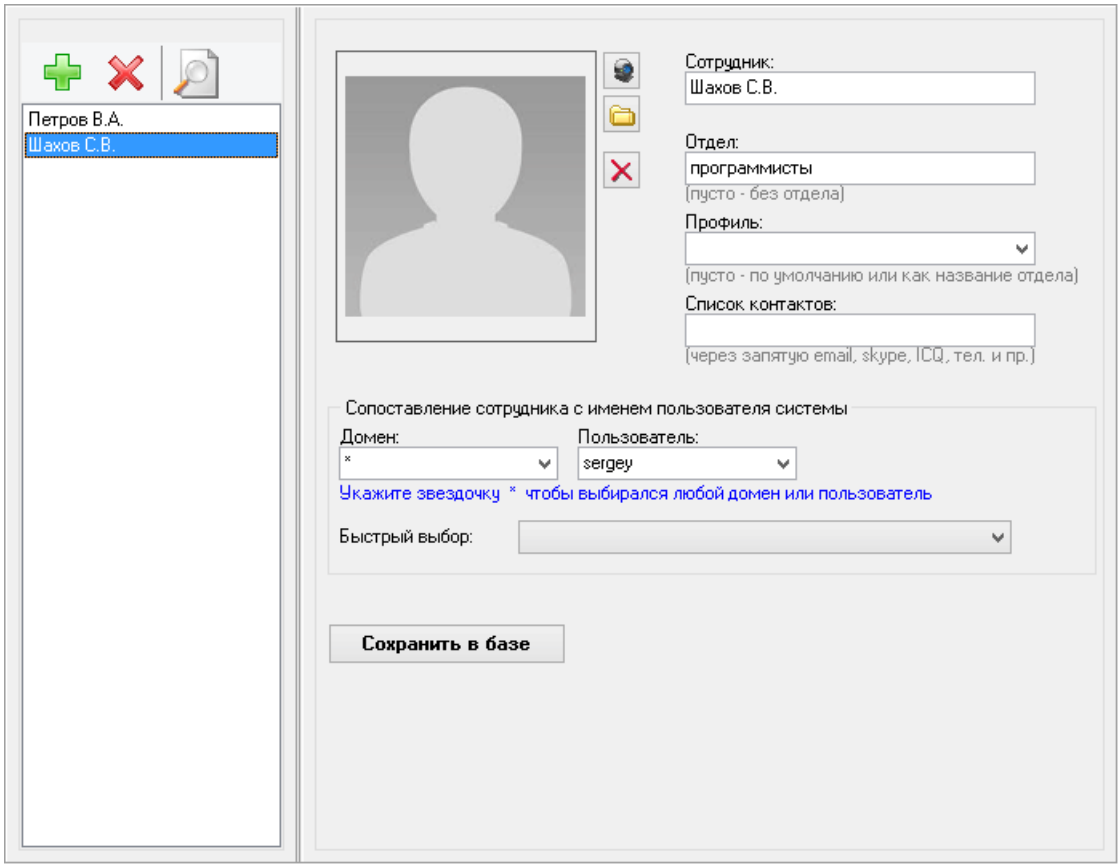
Не забудьте нажать **"Сохранить в базе"** для применения сделанных вами настроек!

Внимание! Права на сохранение структуры есть только у **администратора** базы данных!



6.4. Досье сотрудников

На этой странице можно опционально создавать досье на каждого сотрудника, чтобы в БОСС-Онлайн и БОСС-Оффлайн видеть привычные фамилии вместо имен пользователей системы.



Отдел
Используется для сортировки и отображения в списках БОСС-Оффлайн/БОСС-Онлайн.

Профиль
Нужен для отчета **анализатора**. Вы можете сопоставить сотрудника с конкретным профилем для анализатора.
Если этого не сделать и оставить поле **пустым**, то профиль при построении отчета будет выбираться в след. порядке:
- если найден профиль, название которого **совпадает с отделом сотрудника**, то он будет использоваться;
- профиль **"по умолчанию"**.

Список контактов
Можно указать список различных контактов сотрудника через запятую. Используется при построении отчета "Контакты" и при отправке отчетов самим сотрудникам.

Сопоставление сотрудника с именем пользователя в системе
Для домена или пользователя можно ставить "*" (без кавычек) чтобы это поле игнорировалось.

Не забудьте нажать **"Сохранить в базе"** для применения сделанных вами настроек!

6.5. Синхронизация с Active Directory

Синхронизация предназначена для автоматического поддержания всех данных сотрудников и компании, сохраняемых в настройках комплекса, в актуальном состоянии. Все сделано таким образом, чтобы администраторы не выполняли двойную работу при изменении данных в Active Directory - не будет необходимости изменять эти данные в настройках комплекса. Примеры: уволился или добавился сотрудник, изменилась структура компании, добавились подчиненные у начальников и т.д.
Настроив автоматическую синхронизацию один раз, администратору не нужно будет посещать вкладки настроек "Пользователи базы", "Структура компании", "Досье сотрудников" - синхронизатор все будет выполнять сам автоматически (получая данные из Active Directory и записывая их в базу настроек комплекса).

Важно:
- Синхронизация возможна только при использовании **Microsoft SQL Server** (**MySQL не поддерживается!**).
- Настройки синхронизации, также как и саму синхронизацию, администратор может проводить со своей машины, которая входит или не входит в один из доменов компании.
- Если в компании несколько администраторов, то каждый может работать со своей машины.
- Вход в программу глобальных настроек может быть выполнен под администратором БД или же специально созданным пользователем через меню "Утилиты".
- Необходима учетная запись в домене, которая имеет права на чтение из Active Directory.
- Если в ходе синхронизации необходимо синхронизировать установки клиентских машин, то машина, с которой выполняется синхронизация, должна быть в домене, а также учетная запись в домене должна дополнительно иметь права на копирование файлов, запись в реестр и запуск служб на удаленных машинах домена.
- При удаленном доступе к контроллеру домена необходимо открыть на нем порт LDAP (обычно TCP 389).

Вкладка "Вход"

Если пользователь Windows, под которым осуществлен запуск программы глобальных настроек, не имеет в домене нужных прав для осуществления синхронизации, то можно указать параметры входа в домен на этой вкладке.

Вкладка "Домены"

Здесь указывается список доменов компании, с которыми необходимо производить синхронизацию.
Между доменами должно быть установлено доверие (Trust).
Контроллер домена не является обязательным для указания (обязателен только при удаленном доступе).
Сервер комплекса может быть один для всех доменов или разный (в случае использования нескольких серверов).

Вкладка "Объекты"

Здесь указываются группы, OU или одиночные компьютеры/пользователи для двух типов синхронизации:

1) Синхронизация клиентских установок - указываются группы/машины, на которые должен быть установлен клиент комплекса. Таким образом, в ходе синхронизации происходит установка клиентов на те машины, где клиент еще не установлен. Автоматическое удаление клиентов также возможно, однако управляется настройкой на вкладке настроек **"Общие настройки"** для компьютера. Там же находится и опция **автоматического обновления** клиентов.

2) Синхронизация прав начальников - указываются группы/пользователи в одной из ролей (см. ниже).
Роли начальников:
"Супервизор" - данному начальнику доступны отчеты по всем сотрудникам компании (все домены).
"Суперпользователь" - доступны отчеты только по сотрудникам своего домена.
"Пользователь" - настраиваемые вручную права. После синхронизации на вкладке настроек "Пользователи базы" необходимо самостоятельно выбрать отделы или сотрудников, за которыми будет наблюдать данный начальник.
"Начальник" - доступны отчеты по себе самому и своим подчиненным. Что это означает? Если для каких-то сотрудников в AD установлен **"Manager"** (начальник), то у этого начальника появится поле **directReports**, которое и будет использоваться для создания прав доступа. Т.е. данный начальник сможет наблюдать **только за самим собой, своими подчиненными и подчиненными своих подчиненных (и т.д. рекурсивно по иерархии подчинения вниз)**.

Приоритеты ролей: если один начальник входит сразу в несколько ролей, то для решения данного конфликта приоритеты расставлены в вышеописанном порядке.
В ходе синхронизации происходит заполнение данных на вкладке **"Пользователи базы"**.

Внимание! Стандартные группы **"Компьютеры домена"** и **"Пользователи домена"** использовать нельзя! Вместо этого нужно указывать сам домен в таком же формате (DC=...,DC=...).

Вкладка "Профили"

Аналогично предыдущей вкладке "Объекты", но только указываются группы, OU или одиночные компьютеры/пользователи для сопоставления их с профилями клиентских настроек. См. раздел **"Группы"** в настройках комплекса.
Данная вкладка служит для того, чтобы не заполнять вручную раздел **"Группы"** в настройках комплекса, а синхронизировать с Active Directory.
Важно! Если пользователь входит в две и более групп, которые выбраны здесь и для которых установлены разные профили настроек, то конечная выборка профиля настроек для этого пользователя будет непредсказуемой!

Вкладка "Отделы"

В больших компаниях может быть необходимо выполнять синхронизацию только лишь с выбранными отделами/подразделениями в AD, а не со всей иерархией. В таком случае необходимо выбрать нужные контейнеры AD на этой вкладке (выбранный отдел автоматически включит все отделы нижнего уровня!). Если же данный список пуст, то синхронизация будет производиться полностью по всей иерархии домена(ов).

Вкладка "Клиентские машины"

Здесь можно посмотреть список машин, на которые уже установлен клиент и тех машин, на которые должен быть установлен клиент, но еще не установлен.
Существует возможность вручную выбрать и установить клиентов на машины.
Удаленная установка осуществляется этим способом.

Вкладка "Настройки"

Здесь настраиваются параметры синхронизации:
"Игнорировать отключенные учетные записи" - если учетная запись компьютера или пользователя AD отключена, то обрабатываться синхронизатором не будет.
"Пинговать машины перед установкой клиента" - рекомендуется для ускорения процесса установки (для выключенных машин).
"Название компании" - используется при синхронизации иерархии как верхний ее уровень.
"Опции синхронизации досье" - указывайте названия полей AD для синхронизации досье.
"Настройки очистки лога" - очистка лога также происходит в ходе синхронизации.

Вкладка "Синхронизация"

Можно выполнить синхронизацию вручную (будет создан новый консольный процесс) или же добавить задание в **планировщик заданий** Windows для автоматической синхронизации по расписанию.
Важно: задание в планировщике должно выполняться от имени **текущего пользователя Windows**!

Вкладка "Лог"

Здесь можно смотреть результаты работы как ручной, так и автоматической синхронизации, а также отслеживать изменения настроек.

Что такое "Синхронизировать отложенный режим"?

Включение данной опции синхронизации будет означать следующее: если после полной синхронизации в базе имеются данные мониторинга для пользователей, которых нет в списках наблюдаемых для других пользователей (обычно начальников), то для таких пользователей устанавливается режим отложенного мониторинга (чтобы не нагружать базу их данными мониторинга в дальнейшем).
См. также справку **"Отложенный мониторинг"**.

Какие параметры не синхронизируются и меняются вручную

После успешной синхронизации можно менять вручную следующие параметры, которые не подлежат синхронизации:
- На вкладке "Пользователи базы" все пользователи с логинами SQL (не логины Windows).
- На вкладке "Пользователи базы" для пользователей с логинами Windows "Базовые права".
- На вкладке "Пользователи базы" для пользователей с логинами Windows "Доп. запреты" для роли "Пользователь".
- На вкладке "Досье сотрудников" все досье пользователей, не входящих в состав домена(ов).
- На вкладке "Досье сотрудников" параметр "Профиль".

Как настроить автоматическую отправку отчетов начальникам/сотрудникам

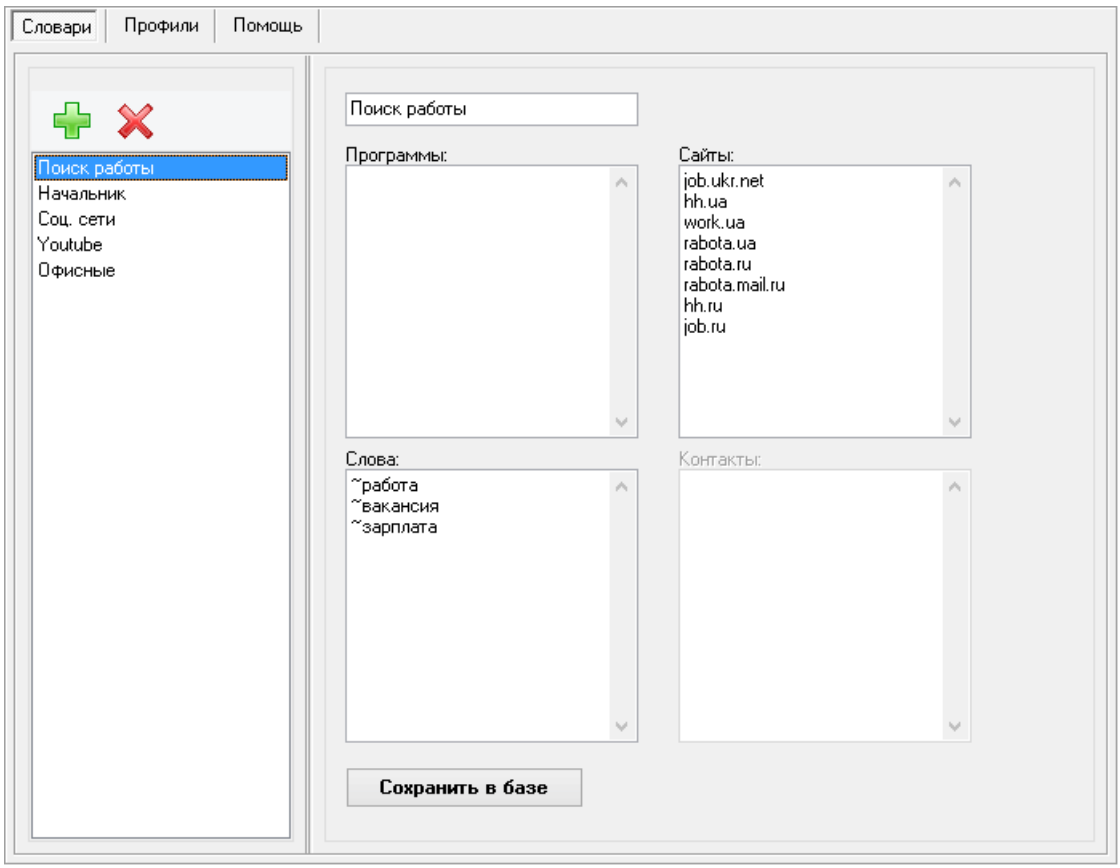
После успешной синхронизации можно вручную настроить права начальникам на отправку отчетов (вкладка **"Пользователи базы"**) если в этом есть необходимость.
Далее эти начальники хотя бы один раз должны зайти в свой **"Личный кабинет"** (через веб-интерфейс БОСС) и включить там авто-генерацию отчетов.
Чтобы сотрудники могли получать отчеты на свои e-mail **о своих же действиях** необходимо указание их e-mail в карточке AD, а также включение соотв. разрешения в правах их начальника (**лучше это разрешение включить у начальника верхнего уровня иерархии подчинения, а не у множества нижестоящих начальников**).
Опции генерации отчетов **должны быть настроены** в серверных настройках (разделы **"Генератор отчетов"**).

6.6. Анализатор рисков и производительности

"Анализатор рисков и производительности" - это интеллектуальный инструмент, автоматически выявляющий возможные риски для компании в повседневной деятельности сотрудников. Это может быть передача критически важных данных конкурентам, поиск нового места работы, снижения производительности труда и т.д. Анализатор рисков проводит сканирование всей ранее собранной информации по деятельности сотрудников и показывает у каких сотрудников есть те или иные риски, а также на основании каких событий эти риски были определены. В контексте анализа производительности сотрудников анализатор наглядно показывает куда именно расходует рабочее время сотрудник и дает возможность оценки "полезности" той или иной работы. Анализатор доступен через БОСС-Оффлайн.

На этой странице настраиваются **Словари** и **Профили** для работы анализатора.

Словари:



Сам словарь не может иметь признака "полезной" или "вредной" активности, т.к. зависит от того, к какому сотруднику будет применен. К примеру, работа в соц. сетях для маркетолога - это не тоже самое что для бухгалтера!
В каждом словаре настраиваются "списки чувствительности". Каждый элемент списка должен быть написан **с новой строки**!
К ним относятся:

1) Программы. Указывайте частичное или полное название программ так, как отображается либо в Диспетчере Задач Windows (колонка "Описание"), либо в отчете "Программы" (в отчете описание указано в кавычках под заголовком окна). Очень редко бывает, что описание для программы не установлено, - для таких случаев нужно указывать частичный или полный путь к exe-файлу программы (путь также необходимо указывать в точности как в отчете "Программы").
Внимание! Если описание для программы присутствует, то нужно указывать описание, а путь к файлу указывать нельзя!
Примеры:
Microsoft Office Word
Photoshop

2) Сайты. Указывайте только домены и поддомены **без префиксов http://, www. и путей**. Если указан домен более верхнего уровня, то будут считаться также и его поддомены (если эти поддомены не указаны отдельно).
Пример: facebook.com

3) Слова. Указывайте одиночные слова (**не фразы!**), к которым будет чувствительность. Если перед словом поставить тильду "~", то будет осуществляться **неточный поиск слова** (с учетом опечаток и особенностей языка).
Не забывайте, что каждое слово указывается **с новой строки!**
Пример: ~начальник

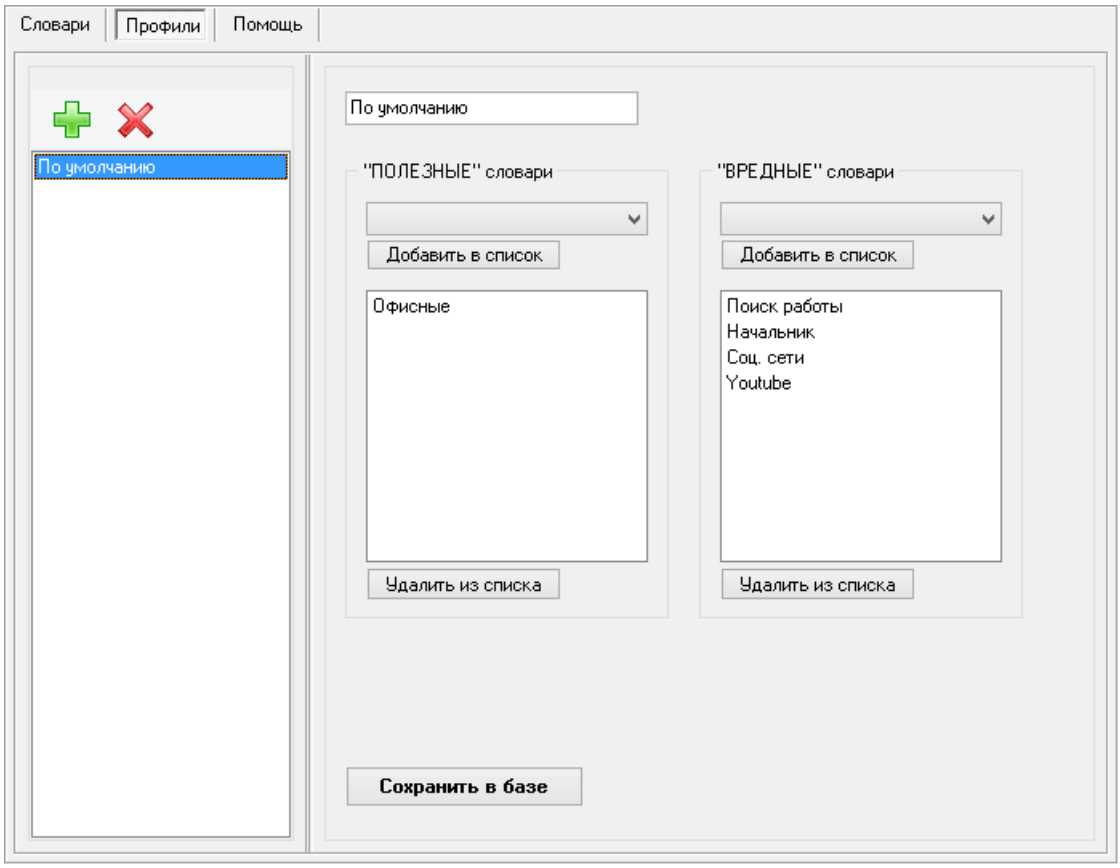
4) Контакты. Укажите список контактов (e-mail, skype, icq, lync, тел. и пр.) **в точности как в отчете "Контакты"**
Пример: petrov@gmail.com

Внимание! Нет смысла размещать один и тот же элемент списка сразу в нескольких словарях (будет использован в

первом словаре).
Внимание! Изменения в словарях вступают в силу только для новых данных наблюдений, которые только будут поступать в базу начиная с этого момента изменения. Т.е. не будет осуществляться пересчет уже накопленных данных из базы по новым словарям!

Не забудьте нажать **"Сохранить в базе"** для применения сделанных вами настроек!

Профили:



Профили включают те или иные словари с признаками **"польза"** или **"вред"**. Причем, не обязательно чтобы все словари были в профиле, - включайте только нужные словари.
Профиль **"По умолчанию"** есть всегда и его нельзя удалить.
Вы можете создавать разные профили исходя из ваших потребностей.
Можно, к примеру, создать по одному профилю для каждого отдела сотрудников.
Чтобы сопоставлять конкретного сотрудника с нужным профилем существует поле **"Профиль" в досье сотрудника**.
Более подробно о выборке профилей для сотрудника см. на вкладке настроек "Досье".

Не забудьте нажать **"Сохранить в базе"** для применения сделанных вами настроек!

6.7. Шаблоны отчетов

Отчет "Поиск"

На этой странице существует возможность создавать шаблоны для отчета поиска информации в базе, чтобы быстро искать пользователей по постоянным критериям.
Можно создать один или несколько шаблонов разных типов.
Для каждого созданного шаблона необходимо добавить критерии поиска, по которым информация будет фильтроваться, при этом можно выбрать сортировку выходного результата, а также условие "И" или "ИЛИ" для объединения критериев поиска.

Важные моменты:
1) При указании имени файла. Можно указать имя файла с или без масок. Однако, если используются маски, то путь к файлу указывать нельзя (разрешено только имя). Если же масок нет, то можно указывать полное или частичное имя файла или пути к нему.
При использовании **цифровых отпечатков** из выпадающего списка можно быстро выбрать конкретный файл для сравнения или указать специальное ***IMPORTANT*** (т.е. проверка на любой файл из списка файлов с цифровыми отпечатками).
2) При указании строк поиска. В этом случае возможны 3 варианта сравнения:
- "совпадает с": полное совпадение;
- "содержит": можно указать часть строки/текста, причем если указать символ **"~" (тильда)** перед **одиночным словом (не текстом!)**, то будет производиться **неточный поиск** данного слова;
- "начинается с": строка начинается с указанной части.
3) Можно не вводить значение сравнения явно, а использовать переменные вида **%название%**, в этом случае соотв. "название" появится в отчете в БОСС-Оффлайн для ввода пользователем. Таким образом, можно каждый раз указывать разные значения не из программы Глобальных настроек, а непосредственно при построении отчетов. Пример:
%Введите имя файла%
Внимание! Переменные **%название%** нельзя использовать при построении отчета поиска через Мастер отчетов. В этом случае шаблоны, содержащие такие переменные, будут исключены из поиска!

Внимание! Если уже запущен БОСС-Оффлайн и производится изменение в переменных **%название%**, то для применения новых значений необходимо перезагрузить страницу БОСС-Оффлайн через выход-вход или нажатие кнопки "Обновить список".

6.8. Цифровые отпечатки

Если содержимое определенных важных файлов компании (с которыми работают сотрудники) меняется редко или не меняется совсем, то имеет смысл снять с этих файлов "цифровые отпечатки" для более удобного поиска операций с ними и получения уведомлений о событиях.

Если добавлять вручную файлы не удобно, то можно настроить автоматическое сканирование и обновление отпечатков (см. здесь)

При использовании цифровых отпечатков нет необходимости добавлять списки чувствительности к тексту в файлах на вкладке DLP, т.к. сравнение происходит быстро по отпечатку файла, а не текстовому содержимому.
Более того, сотрудник может неоднократно **переименовать файл**, однако в отчетах имя файла будет все равно показано оригинальным (для возможности его поиска).
Для одного и того же файла возможно несколько отпечатков (по кол-ву его изменений).

Внимание! Кол-во цифровых отпечатков **ограничено до 200**!

Внимание! Внесенные здесь изменения клиенты получат **спустя 4-5 минут**!

6.9. Тарифы

Вкладка **Тарифы** предназначена для настройки тарифов по различным услугам.

6.10. Списки пользователей

Вкладка **Списки пользователей** предназначена для удаления старых (уже ненужных) записей о местоположении пользователей/компьютеров из базы. Удаленные пользователи и компьютеры не будут отображаться в отчетах **БОСС-Оффлайн**. Не следует путать это удаление с удалением клиентской части с машин сотрудников - **это разные операции**!

6.11. Обслуживание базы

Вкладка **Обслуживание базы** предназначена для ряда оптимизационных работ базы данных.
Если отчеты стали генерироваться значительно медленнее, то имеет смысл запустить переиндексацию базы данных.

6.12. SQL-консоль

Вкладка **SQL-консоль** предназначена для опытных администраторов, чтобы при необходимости выполнять SQL-запросы напрямую к базе данных комплекса.

6.13. Журнал

Вкладка **Журнал** предназначена для просмотра журнала всех входов в программу настроек и БОСС (Онлайн/Оффлайн).

7. Прочее:

7.1. Удаленное наблюдение через интернет

Возможности комплекса СТАХАНОВЕЦ позволяют получать вам все необходимые отчеты мониторинга на ваш e-mail или FTP, чтобы вы были в курсе происходящего в офисе в любой точке мира. Но иногда бывает полезным наблюдать за персоналом "онлайн" или смотреть "свежие" отчеты находясь вне организации.
Ниже будет описано, как нужно настроить сеть, чтобы это стало возможным.

Необходимо открыть **HTTP-порт 80** (его использует программа веб-сервера **\Program Files (x86)\httpd\bin\httpd.exe**) на серверной машине.

Однако в большинстве случаев ваш сервер подключен к интернету через прокси или NAT (в простейшем случае через роутер), потому подключение к реальному IP-адресу по http не сработает. Для решения проблемы необходимо настроить **port-forwarding**, т.е. указать в настройках роутера перенаправлять весь TCP-трафик по http-порту 80 из внешней сети (интернета) на внутренний локальный IP-адрес сервера внутри сети предприятия.
На **этом сайте** вы найдете описание для основных моделей роутеров по настройке port-forwarding.

После того, как все настроено, на любом компьютере или смартфоне запускаете любой браузер и вводите в адресной строке:
http://<DNS_имя_или_IP_сервера>/stkh

Например:
http://95.135.21.16/stkh
или
http://mycompany.org/stkh

О том, как настроить доступ по **https: через SSL** см. здесь

Примечание: на некоторых мобильных устройствах (смартфонах) необходимо вводить IP-адрес, а не имя сервера (если он локальный).

Все!

7.2. Настройка https-доступа

По умолчанию в ходе установки серверной части комплекса происходит автоматическая установка веб-сервера Apache, который изначально настроен на незащищенное соединение по http:// (через порт 80).
Для защищенного соединения через SSL (https://) вам необходимо приобрести **SSL-сертификат** для вашего сервера. Однако, можно также использовать **"самоподписанный"** сертификат, который получается бесплатно (см. ниже).
Для доступа на локальную машину (https://**localhost**) самоподписанный сертификат **автоматически создается** при установке и добавляется в доверенные(*).

Для доступа к **https://your_server_name** нужно:

1) Сгенерировать самоподписанный сертификат.
Необходимо перейти в папку **%ProgramFiles(x86)%\httpd\bin** и в файлах **server.csr.cnf**, **v3.ext** заменить **your_server_name** на DNS-имя вашего сервера. Далее запустить **make_ss_cert.bat** (под **администратором**!).
После этого сгенерированные файлы **server.crt** и **server.key** будут сохранены в **%ProgramFiles(x86)%\httpd\conf**

2) В файле **%ProgramFiles(x86)%\httpd\conf\httpd.conf** необходимо раскомментировать блок:

```
#<VirtualHost *:443>
#    SSLEngine on
#    ServerName your_server_name:443
#    SSLCertificateFile "${SRVROOT}/conf/server.crt"
#    SSLCertificateKeyFile "${SRVROOT}/conf/server.key"
#</VirtualHost>
```

и вместо **your_server_name** указать DNS-имя сервера в точности как и было указано при создании сертификата!

3) **Перезапустить службу Apache**.

4) Далее сертификат нужно добавить в **доверенную зону** на компьютере, с которого будет осуществляться доступ по https:// к серверу. Сделать это можно выполнив команду на данном компьютере (**с правами администратора**)(*), (**):

```
certutil -addstore Root "server.crt"
```

Файл **server.crt** необходимо скопировать с серверной машины (C:\Program Files (x86)\httpd\conf\server.crt).

5) Домен: для добавления сертификата в доверенную зону **в домене** необходимо выполнить такие шаги:
https://technet.microsoft.com/en-us/library/cc754841.aspx

(*) **Внимание!** Для браузера **Firefox** необходимо вручную добавить самоподписанный сертификат в исключения!
(**) **Внимание!** Для браузера **Chrome** необходимо закрыть все окна браузера после добавления сертификата в доверенную зону!

7.3. Перенос сервера

Для переноса сервера комплекса и SQL-базы на другую машину без потери накопленных данных, необходимо выполнить следующие шаги:

1) Через функцию БОСС-Онлайн "Сменить сервер" для всех онлайн-машин указать новую машину сервера (для не онлайн-машин нужно использовать либо удаленную установку с указанием новой машины, либо повторную установку вручную).
Внимание! Если перенос выполняется в нерабочее время и онлайн-машин нет (или их малое кол-во), или же, если данные, которые будут накоплены за время переноса, не критичны, то этот пункт можно выполнить в самом конце процесса переноса сервера.
2) Установить на новой машине SQL-сервер (**версия SQL должна точно совпадать со старой!**).
3) Установить администраторскую часть комплекса на новой машине.
4) Воспользоваться утилитой "Сохранение и восстановление базы данных" в администраторской части комплекса на старой машине для экспорта базы данных в файл (в случае использования MySQL необходимо использовать утилиту mysqldump).
5) Выполнить с помощью этой же утилиты на новой машине импорт базы из ранее экспортированного файла.
6) Запустить утилиту "Начальной конфигурации базы данных" на новой машине.
7) Зайти в глобальные настройки на новой машине и пересоздать всех пользователей базы данных (через первоначальное их удаление).
8) Перенести со старой машины папку теневого копирования и (если есть) папки скриншотов, снимков с веб-камер, аудио. Если **пути на новой машине отличаются**, то необходимо их изменить в настройках "для сервера".
9) Установить сервер комплекса на новой машине.
10) Если использовалась автоматическая генерация отчетов для начальников, то необходимо зайти в "личный кабинет" этих начальников для задания настроек.
11) Повторить пункт 1) для всех остальных машин (если таковые остались).

7.4. Клиентская служба

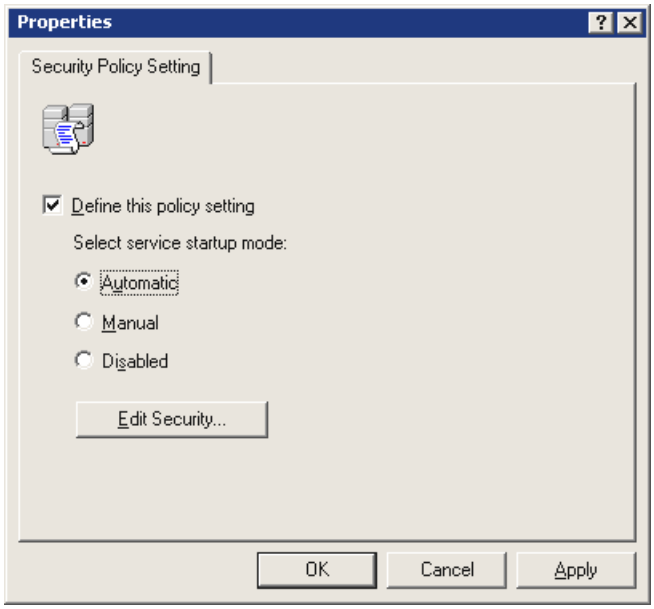
Администратор **домена** может скрыть клиентскую службу от сотрудников, для этого необходимо:

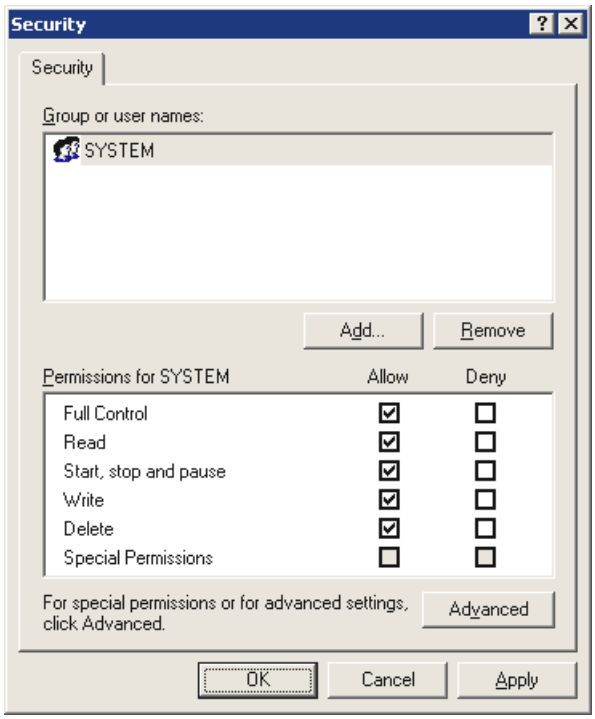
1) Если на контроллере домена не установлена клиентская часть (обычно так и бывает), то временно установить службу-эмулятор с таким же именем, как на клиентах. Для этого нужно получить файл **inst_client.exe** из "Удаленной установки" (способ 4), далее на контроллере домена с правами администратора выполнить в консоли:

```
inst_client.exe -temp -install
```

после чего программа выдаст **имя службы** и статус операции.

2) Запустить редактор **Group Policy Object Editor** существующей групповой политики всего домена или создать новый объект GPO для Organizational Unit (OU), в котором располагаются компьютеры клиентов. В редакторе GPO в разделе **"Computer Configuration" -> ["Policies"] -> "Windows Settings" -> "Security Settings" -> "System Services"** необходимо найти в списке название службы, которую создали на предыдущем шаге (приложение inst_client.exe выдает имя службы).
Для этой службы необходимо изменить политики: установить тип запуска **Automatic**, а также убрать из прав доступа группы **Administrators** и **Interactive**, оставив только **System**:





3) Удалить службу-эмулятор:

```
inst_client.exe -temp -uninstall
```

4) Чтобы не дожидаться применения групповых политик после перезагрузки клиентских машин, можно выполнить

удаленно:

```
gpupdate /force
```

или же воспользоваться **Group Policy Management Console (GPMC)** для удаленного обновления. Подробнее здесь.

Внимание! Служба исчезнет из списка на клиентской машине если уже была установлена на момент применения политик, если же будет установлена позже, то для скрытия необходимо следующее обновление групповых политик на этой машине уже после установки клиентской части.

8. Вопросы и ответы (FAQ):

8.1. Вопросы лицензирования

Каковы ограничения демо-версии?
Вы можете полнофункционально работать только с тремя клиентскими машинами.

Каковы ограничения триал-версии?
Вы можете полнофункционально работать с 50-ю клиентскими машинами не более 2-х недель.

Как быстро я получу ключи после оплаты?
Зависит от способа оплаты. Обычно в течение рабочего дня. Более подробно об этом написано в инструкции, которая вам будет отправлена после оформления заказа.

Получу ли я лицензионное соглашение в бумажном виде о легальности покупки?
Да, конечно. Выписывается по вашему желанию.

Можно ли докупить лицензии к уже имеющимся?
Конечно. При заполнении формы заказа выбираете "Докупить".

Бесплатны ли выходящие обновления?
Да, но только в пределах одной версии N.xx

Бесплатны ли MSSQL_Express и MySQL?
Да, бесплатны.

8.2. Общие вопросы

Нужен ли выделенный сервер для работы ПО?
Да, нужен. Однако допускаются временные перерывы в его работе. В остальное же время он должен быть включен постоянно (или хотя бы во время работы сотрудников).
Также это может быть и машина администратора, если нет выделенной.

Не нарушает ли программа права человека?
Нет. В программе по умолчанию включен режим открытого наблюдения с выдачей сообщения пользователю, в котором указано, что за ним ведется наблюдение.

Передает ли программа в базу личные пароли и номера кредитных карточек пользователей?
Опционально.

8.3. Технические вопросы

Почему не отображаются русские буквы в программе?
В языковых настройках системы нужно выбрать язык по умолчанию (для не-Unicode программ) одним из славянских, а также правильно выбрать свое местоположение и региональные стандарты.
Для клиентской части это не требуется.

Как установить новую версию клиента сразу на все машины?
См. раздел "обновление ПО"

Как будет работать клиентская часть при выключенном сервере/SQL-базе?
Клиент постоянно пытается поддерживать связь с сервером, но может и кешировать данные при необходимости (т.е. работать без сервера).

Утерян пароль администратора базы данных. Что делать?
Используйте утилиту восстановления и сохранения базы данных в администраторской части ПО.

При использовании терминального сервера устанавливать клиентскую часть нужно на всех пользователей?
Нет. Устанавливается один раз под администратором.

Устанавливается ли клиентская часть на каждого пользователя системы индивидуально?
Нет. Устанавливается один раз под администратором на данной машине.

MySQL ниже 5.0.27 в ПО не поддерживается, а мы не можем обновить наш сервер. Что делать?
Просто установите новую версию сервера как вторую инстанцию (см. справку в разделе "Установка SQL-сервера").

Почему не работает мониторинг распечатанных документов?
См. справку на странице настроек мониторинга принтера в программе настроек администраторской части.

Не могу зайти с мобильного смартфона на веб-сервер. Почему?
На некоторых мобильных устройствах необходимо в адресной строке браузера вводить IP-адрес, а не имя сервера (если он локальный).

Чем открыть файлы принтера SPL?
См. описание здесь

Как настроить доступ к веб через https (SSL)?
см. здесь

Почему некоторые программы стали выдавать предупреждение о ненадежном корневом сертификате?
см. здесь

Используем антивирус. Почему после установки клиента пропал Интернет?
см. здесь