|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | | | |
|  |  |  | | **УТВЕРЖДАЮ** Генеральный директор  ООО «Кейсистемс»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А. А. Матросов  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. | |
|  |  | сервисная служба  «сервис авторизации и единого управления учетными записями»  версия  Руководство пользователя  Лист утверждения  **Р.КС. 01120‑01 34 00‑ЛУ** | | | |
|  |  |
|  |  |
|  |  |
| Подп и дата |  |
|  | | **СОГЛАСОВАНО**  Заместитель генерального директора  ООО «Кейсистемс»  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Е. В. Фёдоров  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. | |
| Инв.N дубл |  |
| Взам.инв.N |  |  | | Руководитель ДПиРСИБ  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д. В. Галкин  «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2014 г. | |
|  | |  | |
| Подп и дата |  |
|  | |  | |
|  | | | |
| Инв.N подл |  | 2014 | | | |
|  |  | | Литера А |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | | | |
|  |  |  | |  | |
|  |  | сервисная служба  «сервис авторизации и единого управления учетными записями»  версия  Руководство пользователя  **Р.КС. 01120‑01 34 00**  Листов 31 | | | |
|  |  |
|  |  |
|  |  |
| Подп и дата |  |
|  | |  | |
| Инв.N дубл |  |
| Взам.инв.N |  |  | |  | |
|  | |  | |
| Подп и дата |  |
|  | |  | |
|  | | | |
| Инв.N подл |  | 2014 | | | |
|  |  | | Литера А |

АННОТАЦИЯ

Настоящий документ является руководством пользователя сервисной службы «Сервис авторизации», предназначенной для интеграции учетных записей пользователей в различных программных комплексах и содержит описание операций по созданию и редактированию учетных записей пользователей. Реализация соответствует методическому документу «Меры защиты информации в государственных информационных системах» (утв. Федеральной службой по техническому и экспортному контролю 11 февраля 2014 г.).

Руководство состоит их двух разделов:

* Описание операций.
* Рекомендации по освоению.

Раздел «Описание операций» содержит описание операций технологического процесса.

Раздел «Рекомендации по освоению» содержит рекомендации и ответы на часто возникающие вопросы.

СОДЕРЖАНИЕ

[Введение 4](#_Toc398214407)

[1. Описание операций 5](#_Toc398214408)

[1.1. Сервис авторизации 5](#_Toc398214409)

[1.1.1. Активация комплекса 5](#_Toc398214410)

[1.1.2. Вход в администрирование СА 7](#_Toc398214411)

[1.1.3. Список пользователей 7](#_Toc398214412)

[1.1.4. Порядок создания учетной записи пользователя 9](#_Toc398214413)

[1.1.4.1. Ручной ввод параметров учетной записи 9](#_Toc398214414)

[1.1.4.2. Импорт учетных записей пользователей 11](#_Toc398214415)

[1.1.5. Удаление учетных записей пользователей 12](#_Toc398214416)

[1.1.6. Пользователи и комплексы 12](#_Toc398214417)

[1.1.7. Комплексы 13](#_Toc398214418)

[1.1.8. Шаблоны 15](#_Toc398214419)

[1.1.8.1. Импорт шаблона 17](#_Toc398214420)

[1.1.9. Настройки 17](#_Toc398214421)

[1.1.10. Сервис 19](#_Toc398214422)

[1.2. Подготовка ПК к работе через СА 20](#_Toc398214423)

[1.2.1. Регистрация менеджера авторизации в прикладном ПК 20](#_Toc398214424)

[1.2.2. Редактирование файла «Web.config» прикладного ПК 21](#_Toc398214425)

[1.2.3. Работа со списком пользователей в прикладном ПК 22](#_Toc398214426)

[1.2.4. Создание шаблона в прикладном ПК 22](#_Toc398214427)

[1.2.5. Экспорт шаблона из прикладного ПК 24](#_Toc398214428)

[1.2.6. Экспорт учетных записей пользователей 25](#_Toc398214429)

[1.3. Работа в ПК через СА 27](#_Toc398214430)

[1.3.1. Вход в программный комплекс через СА 27](#_Toc398214431)

[2. Рекомендации по освоению 28](#_Toc398214432)

[2.1. Настройка сертификатов 28](#_Toc398214433)

[Перечень сокращений 30](#_Toc398214434)

[Лист регистрации изменений 31](#_Toc398214435)

Введение

Настоящее руководство пользователя содержит описание операций по созданию и редактированию учетных записей пользователей при помощи сервисной службы «Сервис авторизации», включая описание этапов регистрации пользовательских данных, выбора доступных прикладных программных комплексов, работы с шаблонами создания учетных записей пользователей.

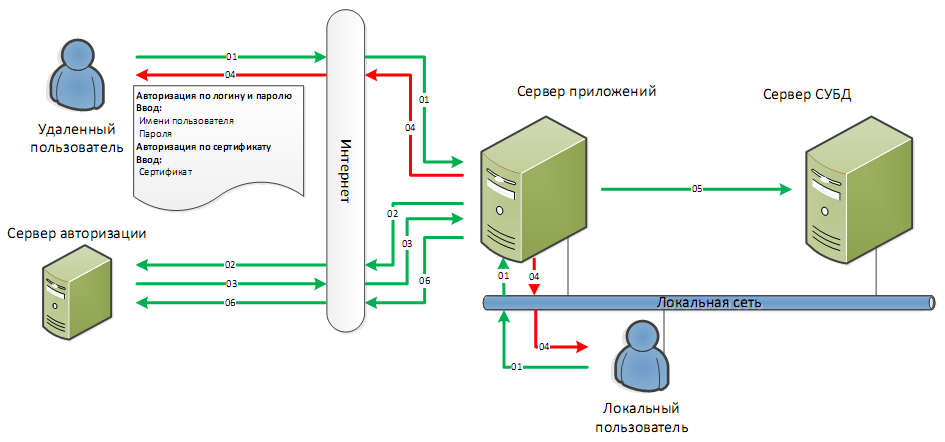
Условные обозначения

В документе используются следующие условные обозначения:

|  |  |  |  |
| --- | --- | --- | --- |
|  | Уведомление | – | Важные сведения о влиянии текущих действий пользователя на выполнение других функций, задач программного комплекса. |
|  | Предупреждение | – | Важные сведения о возможных негативных последствиях действий пользователя. |
|  | Предостережение | – | Критически важные сведения, пренебрежение которыми может привести к ошибкам. |
|  | Замечание | – | Полезные дополнительные сведения, советы, общеизвестные факты и выводы. |
| [Выполнить] | | – | Функциональные экранные кнопки. |
| <F1> | | – | Клавиши клавиатуры. |
| «Чек» | | – | Наименования объектов обработки (режимов). |
| Статус | | – | Названия элементов пользовательского интерфейса. |
| окна => навигатор | | – | Навигация по пунктам меню и режимам. |
| п. 2.1.1  рисунок 5 | | – | Ссылки на структурные элементы, рисунки, таблицы текущего документа, ссылки на другие документы. |

1. Описание операций

Cлужба «Сервис авторизации и единого управления учетными записями» (далее «СА») предназначена для решения задачи интеграции учетных записей пользователей и позволяет создавать, редактировать и хранить единый логин и пароль, действительный для всех указанных в параметрах учетной записи СУБД прикладных программных комплексах. (Рисунок 1).

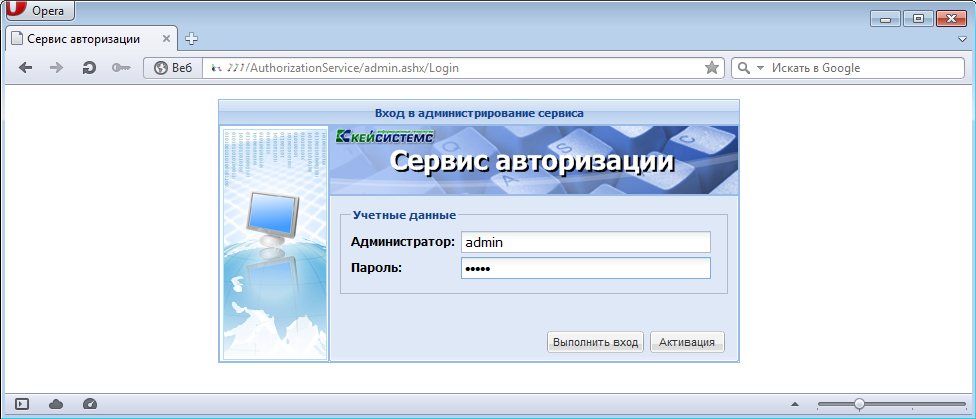


1. . Схема работы СА

На схеме указаны следующие информационные потоки:

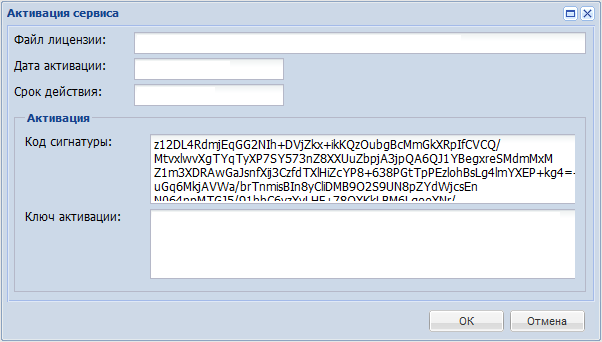
1. Запрос авторизации удаленного\локального пользователя на прикладной сервер приложений.
2. Запрос сервера приложений к серверу авторизации на предмет легитимности авторизуемых учетных данных.
3. Ответ сервера авторизации серверу приложений о легитимности учетных данных для авторизации.
4. Отказ авторизации от сервера приложений конечному пользователю.
5. Авторизация в прикладном комплексе.
6. При необходимости дополнительная синхронизация данных между сервером приложений и сервером авторизации, после успешной авторизации.
   1. Сервис авторизации
      1. Активация комплекса

Для работы с СА не требуется установки каких-либо компонентов, достаточно стандартного Internet-браузера. Введите в адресной строке адрес СА, в открывшемся окне введите имя пользователя и пароль учетной записи администратора СА и нажмите кнопку [Активация] (Рисунок 5).



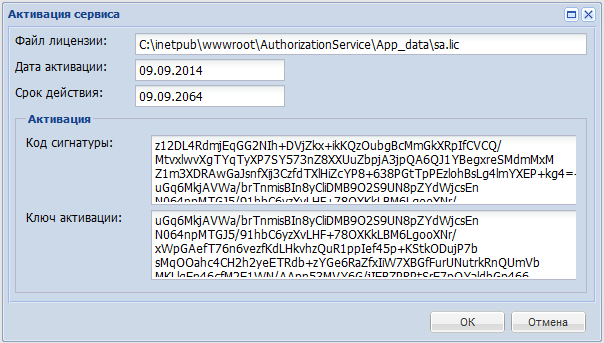
1. . Окно авторизации СА

В открывшемся окне активации СА скопируйте содержимое поля (Рисунок 6)



1. . Получение кода сигнатуры для активации

Далее перейдите в [Личный кабинет](http://portal.keysystems.ru/) на Сайте компании и получите код активации по данному коду сигнатуры. Полученный ключ введите в поле Ключ активации и нажмите кнопку [ОК] (см. Рисунок 6).

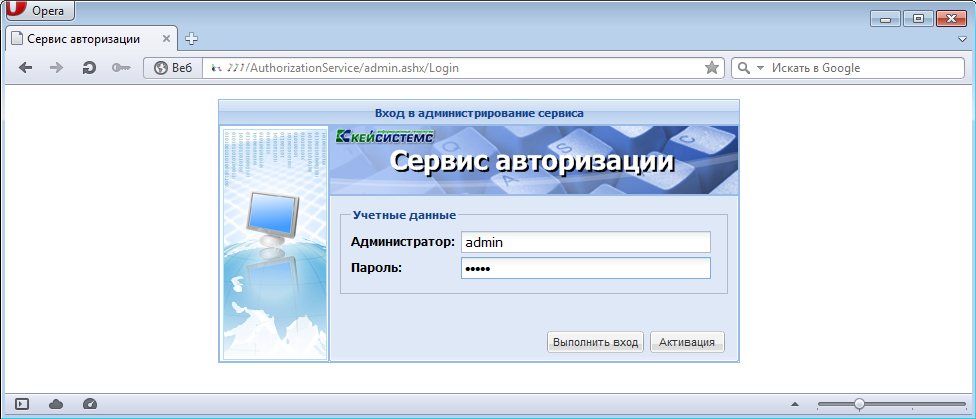


1. . Активация СА

В результате активации будут заполнены остальные поля окна активации СА (см. Рисунок 4) и станет возможным вход под учетной записью администратора.

* + 1. Вход в администрирование СА

Введите в адресной строке адрес СА, в открывшемся окне введите имя пользователя и пароль учетной записи администратора СА (Рисунок 5).



1. 5. Вход в администрирование СА

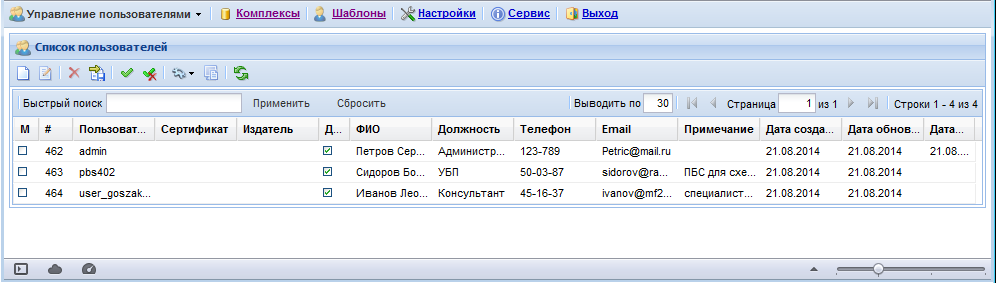
По кнопке [Выполнить вход] откроется окно администрирования СА.

* + 1. Список пользователей

В главном меню выберите строку «Пользователи» в раскрывающемся списке пункта меню  «Управление пользователями».

Меню => Управление пользователями => Пользователи

Откроется список зарегистрированных пользователей (Рисунок 6).

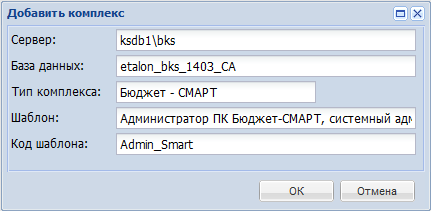


1. . Список пользователей

В режиме списка доступны следующие действия:

* создание новой учетной записи по кнопке  Создать (п. 1.1.4.1);
* редактирование существующей записи по кнопке  Редактировать;
* удаление записи по кнопке  **Удалить** (п. 1.1.5);
* импорт учетных записей по кнопке  Импорт (п. 1.1.4.2);
* установка отметок учетных записей по кнопке  Отметить все;
* снятие отметок по кнопке  **Разметить все**;
* выполнение следующего ряда действий по кнопке  Сервис:
* блокировка пользователя во всех прикладных ПК (глобальная) по ссылке  Заблокировать пользователя;
* установка принудительной смены пароля по ссылке Сменить пароль при следующем входе;
* включение режима «доверенного пароля», который пользователь введет в окне логина при первом входе в ПК через СА по ссылке Установить режим доверенного пароля (введенный пароль будет установлен как пароль пользователя на СА, после чего режим будет автоматически отключен);
* смена типа авторизации, выбираемого из значений «по логину/паролю» и «по сертификату» по ссылке Сменить тип авторизации;
* добавление прикладного программного комплекса по ссылке  Добавить комплекс (Рисунок 7).

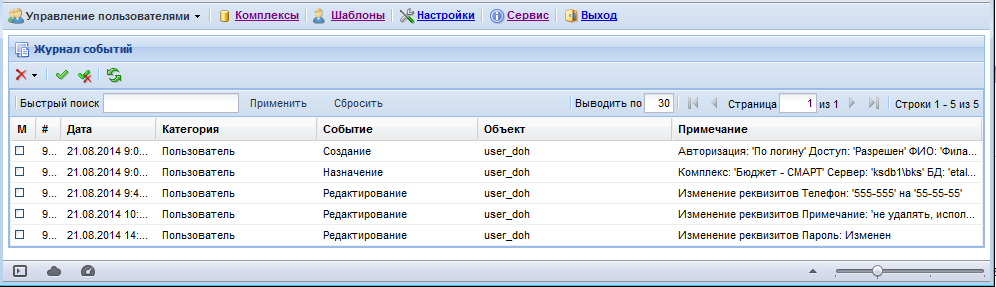
|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Для добавления ПК отметьте нужную строку в списке учетных записей пользователей (см. Рисунок 6), затем выберите строку  Добавить комплекс в раскрывающемся списке инструмента  Сервис и в окне добавления комплекса заполните соответствующие реквизиты (Рисунок 7). |  |
|  |  |  |



1. . Добавление прикладного ПК для выбранного пользователя

* Обновление списка по кнопке  Обновить.
* Просмотр журнала событий по кнопке  Журнал событий.

Перейдите к окну просмотра журнала событий в новой вкладке для отмеченной в списке учетной записи пользователя (Рисунок 8).

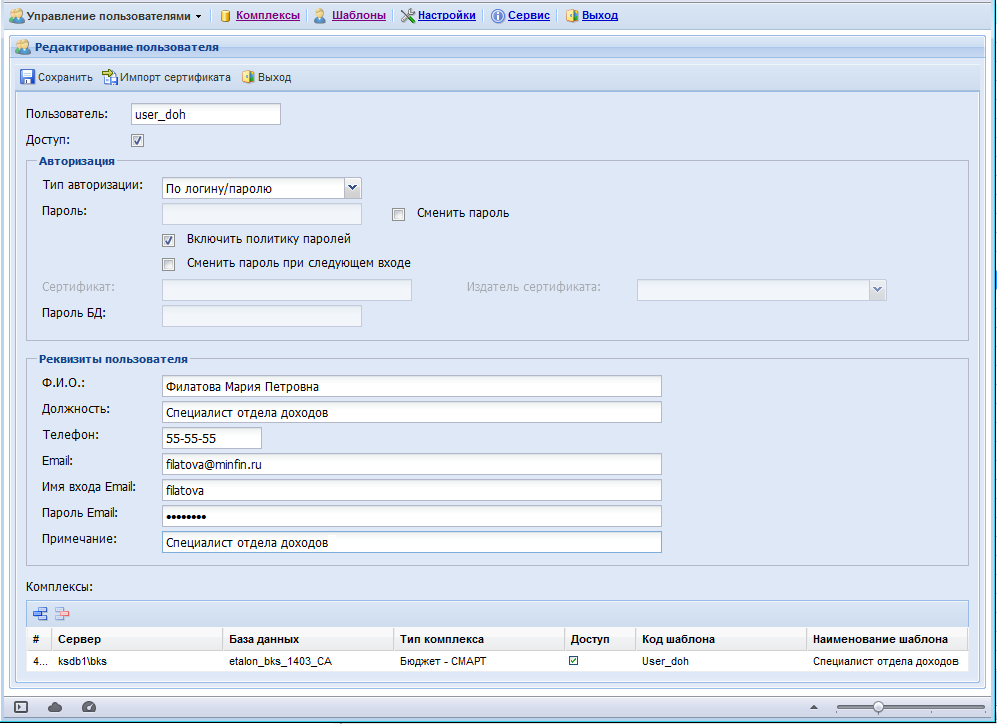


1. . Просмотр журнала событий для выбранного пользователя

В журнале событий сохраняются все действия, выполненные над учетной записью данного пользователя.

* + 1. Порядок создания учетной записи пользователя
       1. Ручной ввод параметров учетной записи

Создание учетной записи пользователя осуществляется по кнопке  Создать панели инструментов списка пользователей (см. Рисунок 6). Откроется окно добавления/редактирования параметров учетной записи пользователя (Рисунок 9).



1. . Окно регистрации пользователя

В окне редактирования реквизитов учетной записи пользователя заполните следующие поля:

Пользователь – введите имя пользователя;

Доступ – при отсутствии флажка в данном поле пользователю будет заблокирован доступ во все прикладные ПК (глобальная настройка доступа).

Группа «Авторизация»

Тип авторизации – выберите одно из двух возможных значений для авторизации:

* «По логину/паролю» – вход в СА и прикладные ПК для данного пользователя будет осуществляться стандартным способом: по комбинации логин/пароль.
* «По сертификату» – при входе будет проверяться сертификат пользователя.

Пароль – введите пароль пользователя (с учетом значений настроек п. меню «Настройки», если включена настройка «Включить политику паролей».

Включить политику паролей – включение учета условий политики паролей, действующих на момент регистрации данного пользователя (п. 1.1.9). Политика паролей накладывает определенные условия на количество символов в пароле, условия изменения пароля и установи блокировки при входе. Например, при использовании политики «не единых» паролей осуществляется автоматическая блокировка несанкционированного доступа при попытке пользователя, отключив сервис авторизации, зайти в БД напрямую.

Сменить пароль при следующем входе – при установке флажка пользователю будет предложено сменить пароль при следующем входе.

Сертификат – наименование сертификата пользователя при выборе в поле Тип авторизации значения «По сертификату».

Издатель сертификата – выберите организацию - издателя в раскрывающемся списке.

Пароль БД – пароль, под которым пользователь сможет войти в БД, отключив СА, если в настройке «Единое имя входа и пароль» (п. 1.1.9) установлено значение «Нет», при установленном значении «Да» настройки, данное поле будет недоступно для ввода, и в нем будет автоматически дублироваться значение поля «Пароль».

Группа «Реквизиты пользователя»

Ф.И.О. – укажите фамилию, имя и отчество пользователя.

Должность – укажите должность, занимаемую пользователем в организации.

Телефон – укажите номер телефона пользователя.

Email – укажите адрес электронной почты пользователя, который будет использоваться при отправке сообщений.

Имя входа Email – укажите имя пользователя для входа по указанному почтовому адресу.

Пароль Email – укажите пароль пользователя для входа по указанному почтовому адресу.

Группа «Комплексы»

В табличной части окна редактирования осуществляется добавление/удаление прикладных ПК, которые будут доступны данному пользователю для работы.

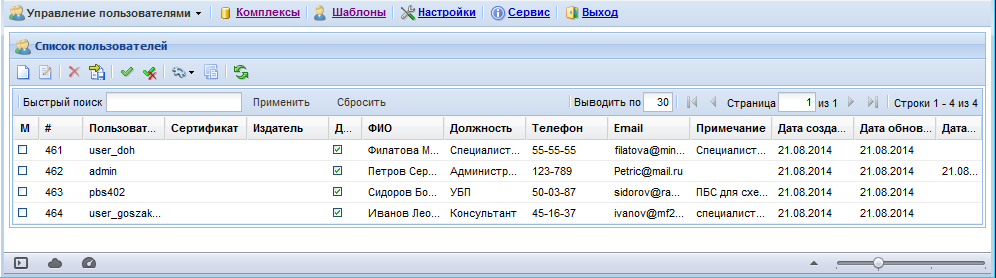
По кнопке  Добавить строку добавляется новая строка для указания прикладного ПК (п. 1.1.7) и шаблона прав доступа (п. 1.1.8), доступного пользователю под текущей учетной записью.

По кнопке  Удалить строку осуществляется удаление выбранной строки записи о доступном комплексе.

Для добавления доступного комплекса выбирается связка «сервер - база данных - тип комплекса» из значений, сохраненных в режиме «Комплексы» (п. 1.1.7). Далее выбирается код - наименование шаблона из значений, сохраненных в режиме «Шаблоны» (п. 1.1.8).

Доступ – при отсутствии флажка в какой-либо строке списка пользователю будет заблокирован доступ в соответствующий прикладной ПК (локальная настройка доступа).

Сохранение учетной записи осуществляется по кнопке  Сохранить. Сохраненная учетная запись отобразится в списке пользователей (Рисунок 10).



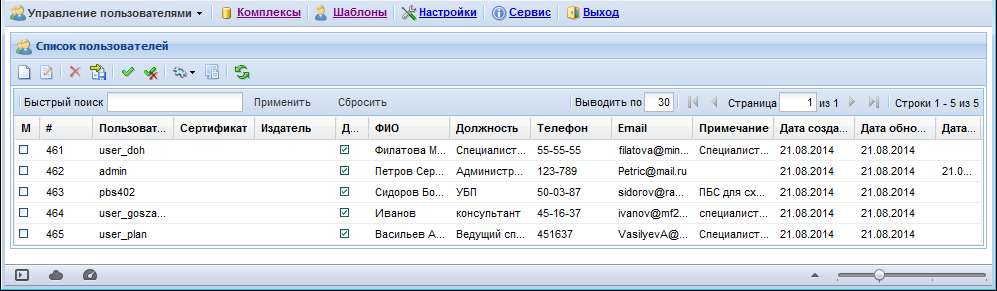
1. . Обновленный список пользователей
   * + 1. Импорт учетных записей пользователей

Доступен также импорт учетных записей пользователей из файла, выгруженного из соответствующего ПК. Процедура предварительного экспорта описана в п.1.2.6.

Для последующего импорта учетных записей из файла нажмите кнопку  Импорт панели инструментов списка пользователей (см. Рисунок 10).

В окне импорта нажмите кнопку [Browse…]. Выберите файл импорта в каталоге размещения и нажмите кнопку [Открыть].

По кнопке [ Импорт] учетные записи из файла будут импортированы и отобразятся в окне списка пользователей (Рисунок 11).



1. . Окно списка пользователей с импортированными учетными записями

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Импорт осуществляется с учетом шаблонов создания учетных записей, привязанных при экспорте учетных записей пользователей из прикладного ПК. Поэтому перед импортом учетных записей пользователей следует убедиться в наличии данных шаблонов на СА. При отсутствии шаблонов необходимо осуществить их импорт (п. 1.1.8.1) до импорта учетных записей пользователей. |  |
|  |  |  |

* + 1. Удаление учетных записей пользователей

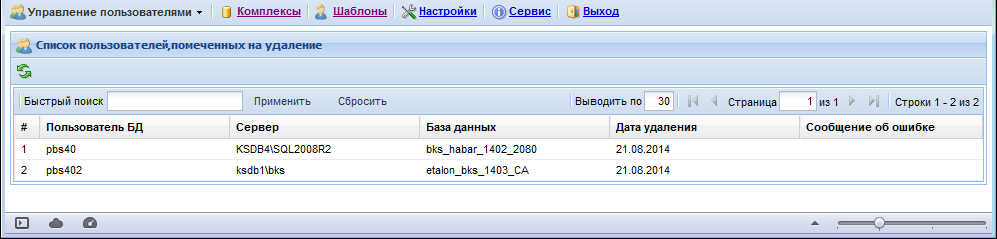
В главном меню выберите строку «Пользователи» в раскрывающемся списке пункта меню  «Управление пользователями».

Меню => Управление пользователями => Пользователи

Откроется список зарегистрированных пользователей (Рисунок 6).

Выберите в списке пользователей учетные записи для удаления и нажмите кнопку  Удалить панели инструментов. При этом выбранные записи будут помечены к удалению и перестанут отображаться в общем списке пользователей.

Просмотр таких записей осуществляется путем выбора строки  «Помеченные на удаление» в раскрывающемся списке пункта меню  «Управление пользователями» (Рисунок 12).



1. . Список пользователей для удаления

При входе какого-либо пользователя в прикладной программный комплекс будут проанализированы возможности удаления отмеченных в списке СА пользователей. Например, пользователь ПК «Бюджет-СМАРТ» не может быть удален при условии, что он является исполнителем на каком-либо этапе маршрута бизнес-процесса.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Удаление учетной записи пользователя, которая ни разу не использовалась для входа ни в один из назначенных прикладных ПК, осуществляется одноэтапно, без переноса в «Список пользователей, помеченных на удаление».  Удаление учетной записи пользователя нескольких прикладных ПК осуществляется после входа какого-либо пользователя в каждый из назначенных ему комплексов. |  |
|  |  |  |

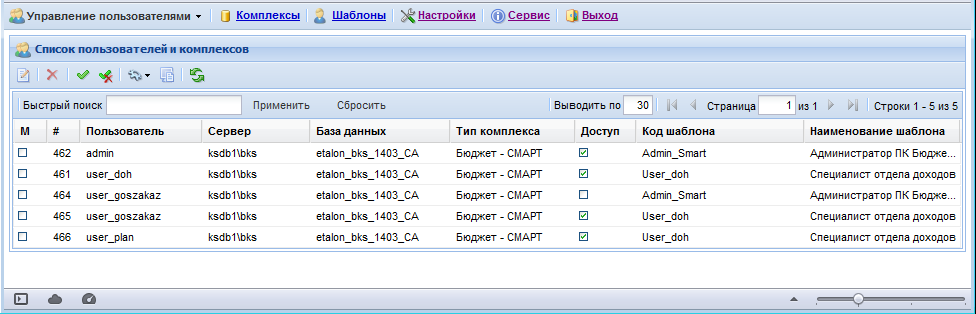
* + 1. Пользователи и комплексы

В главном меню выберите строку «Пользователи и комплексы» в раскрывающемся списке пункта меню  «Управление пользователями».

Меню => Управление пользователями => Пользователи и комплексы

Откроется список зарегистрированных пользователей, причем количество отображения каждой из учетных записей будет соответствовать количеству назначенных каждому прикладных ПК (Рисунок 13).

Из данного режима доступен стандартный переход к окну редактирования параметров учетной записи пользователя по кнопке  Редактировать, удаление назначенного прикладного ПК путем удаления соответствующей строки списка по кнопке  Удалить, также доступна блокировка назначенного прикладного ПК по ссылке  Заблокировать комплекс в раскрывающемся списке кнопки  Сервис.

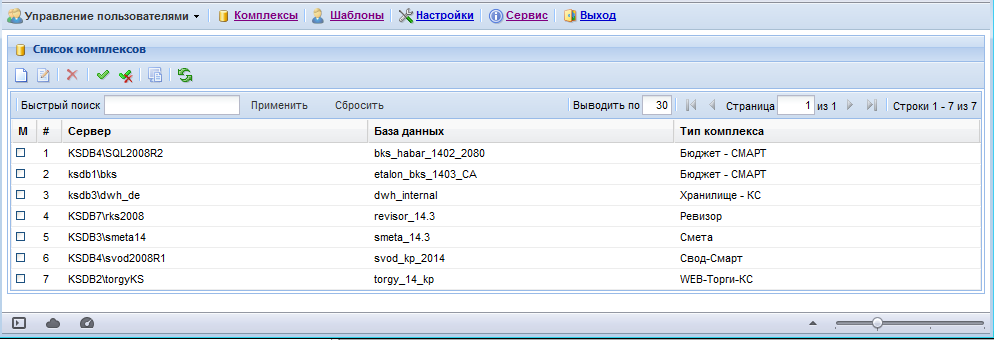


1. . Пользователи и комплексы
   * 1. Комплексы

Выберите пункт меню «Комплексы».

Меню => Комплексы

В окне списка прикладных ПК отобразятся наименования подключенных баз данных с указанием серверов и типов комплексов (Рисунок 14).



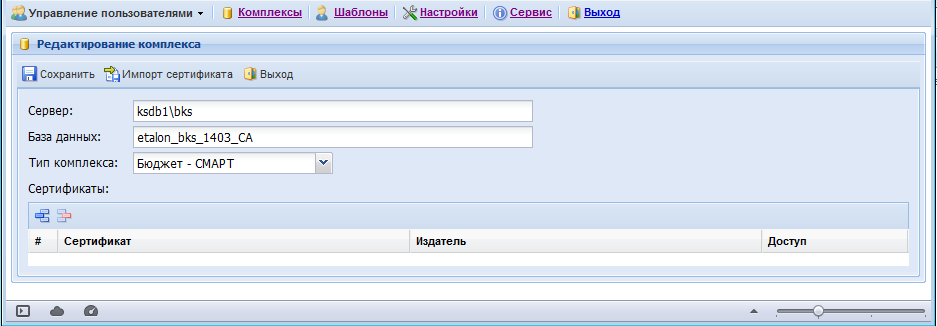
1. . Список прикладных ПК

В окне списка прикладных ПК доступен следующий набор действий:

* создание новой записи по кнопке  Создать;
* редактирование существующей записи по кнопке  Редактировать;
* удаление записи по кнопке  **Удалить** (п. 1.1.5);
* импорт учетных записей по кнопке  Импорт (п. 1.1.4.2);
* установка отметок записей по кнопке  Отметить все;
* снятие отметок по кнопке  **Разметить все**;
* просмотр журнала событий по кнопке  Журнал событий;
* обновление списка по кнопке  Обновить.

Для подключения новой базы данных прикладного ПК нажмите кнопку  Создать.

Откроется окно добавления/редактирования (Рисунок 15).



1. . Окно добавления/редактирования комплекса

В данном окне заполните следующие поля:

Сервер – имя сервера размещения ПК.

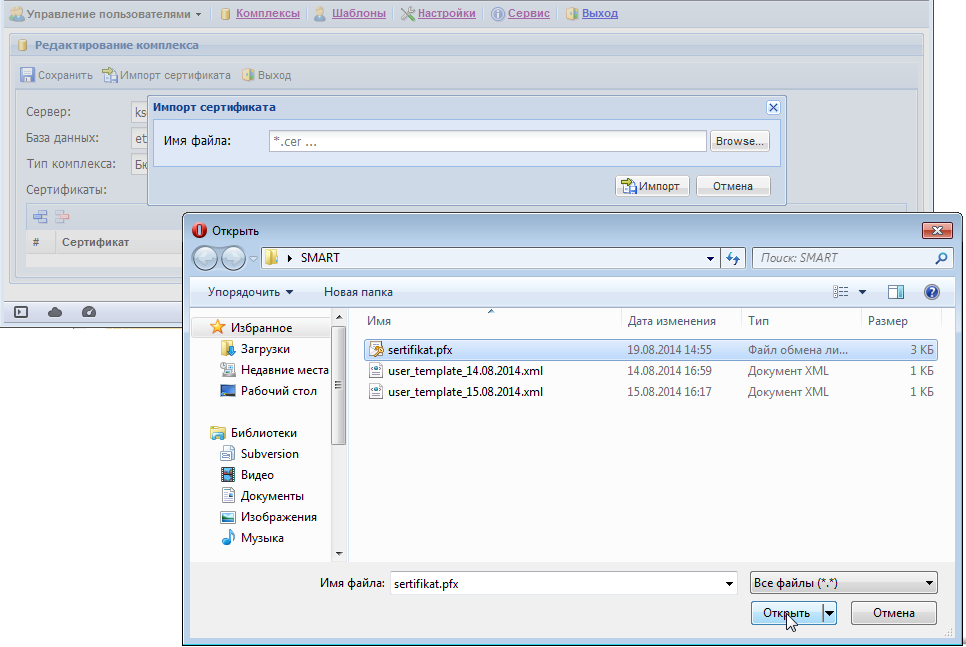
База данных – имя базы данных.

Тип комплекса – тип прикладного ПК выбирается из раскрывающегося списка доступных типов.

Сертификаты – доступен как режим импорта сертификатов сервера приложений, так и режим ручного ввода. Добавление записи в списке сертификатов осуществляется по кнопке  Добавить строку, удаление по конке  Удалить строку. При указании сертификата заполнение поля Издатель обязательно.

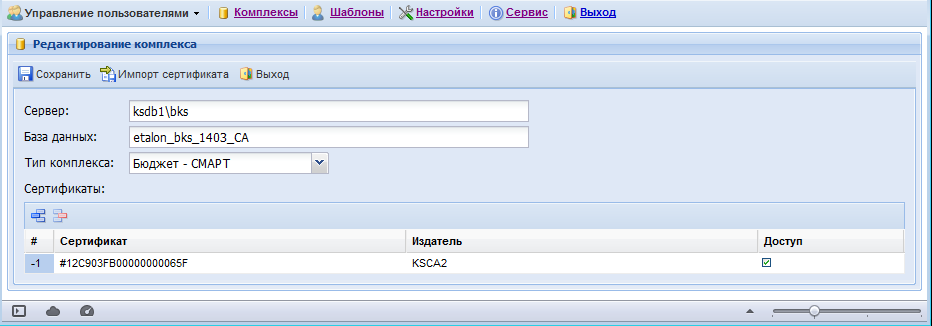
Импорт осуществляется по кнопке  Импорт сертификата панели инструментов окна добавления/редактирования (см. Рисунок 15).

В окне импорта нажмите кнопку [Browse…]. Выберите сертификат в каталоге размещения и нажмите кнопку [Открыть] (Рисунок 16).



1. . Окно выбора сертификата для импорта

Сертификат будет импортирован и отобразится в окне добавления/редактирования комплекса (Рисунок 17).



1. . Окно добавления/редактирования с импортированным сертификатом

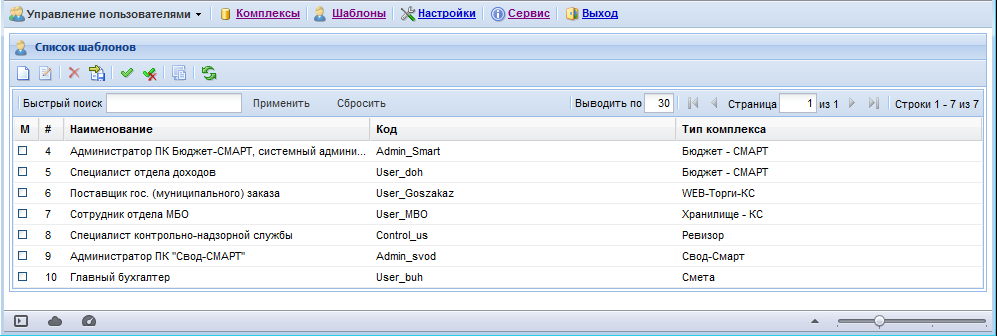
Сохранение всех изменений окна добавления/редактирования комплекса осуществляется по кнопке  Сохранить.

* + 1. Шаблоны

Права доступа пользователя в программном комплексе определяются шаблоном, назначаемым при создании пользователя. Выберите пункт «Шаблоны» главного меню.

Меню => Шаблоны

В окне списка шаблонов отображаются наименования шаблонов, их код и тип комплекса, к которому относится данный шаблон (Рисунок 18).



1. . Список шаблонов

Панель инструментов списка позволяет выполнить следующие действия:

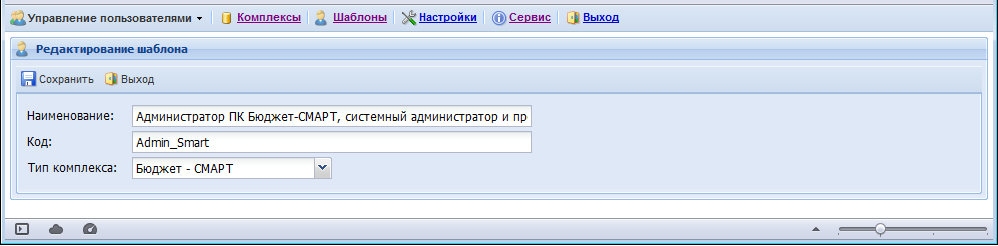
* для создания шаблона нажмите кнопку  Создать;
* для редактирования шаблона нажмите кнопку  Редактировать;
* для удаления одного или нескольких шаблонов выделите нужные записи в списке и нажмите кнопку  Удалить;
* для импорта новых шаблонов нажмите кнопку  Импорт;
* для отметки записей в списке нажмите кнопку  Инверсия;
* для снятия отметок в списке записей нажмите кнопку  Разметить все;
* для перехода к окну просмотра журнала событий по выбранному элементу списка нажмите кнопку  Журнал событий;
* для обновления списка нажмите кнопку  Обновить.

Нажмите кнопку  Создать. В окне добавления/редактирования шаблона заполните следующие поля:

Наименование – наименование шаблона;

Код – код шаблона;

Тип комплекса – выберите в раскрывающемся списке тип программного комплекса, к режимам которого относится данный шаблон.



1. . Окно редактирования шаблона

Сохранение всех изменений окна добавления/редактирования комплекса осуществляется по кнопке  Сохранить.

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Предупреждение: не рекомендуется вводить реквизиты шаблона вручную во избежание ошибок его идентификации при последующем входе пользователя в соответствующий ПК. |  |
|  |  |  |

* + - 1. Импорт шаблона

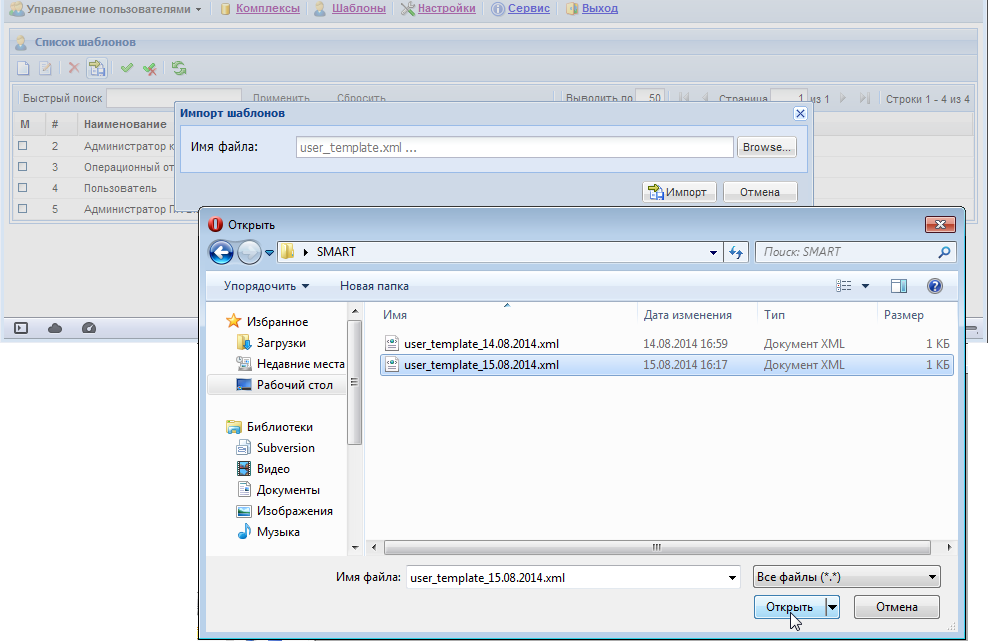
Передача шаблона создания учетных записей из прикладного ПК и сохранение в виде файла описана в п. 1.2.5.

Выберите пункт «Шаблоны» главного меню.

Меню => Шаблоны

На панели инструментов в окне списка шаблонов (см. Рисунок 18) нажмите кнопку  Импорт.

Выберите каталог размещения выгруженных файлов user\_template, выберите нужный файл и нажмите кнопку [Открыть]. В окне «Импорт шаблонов» нажмите кнопку [ Импорт] (Рисунок 20).



1. . Прием шаблонов

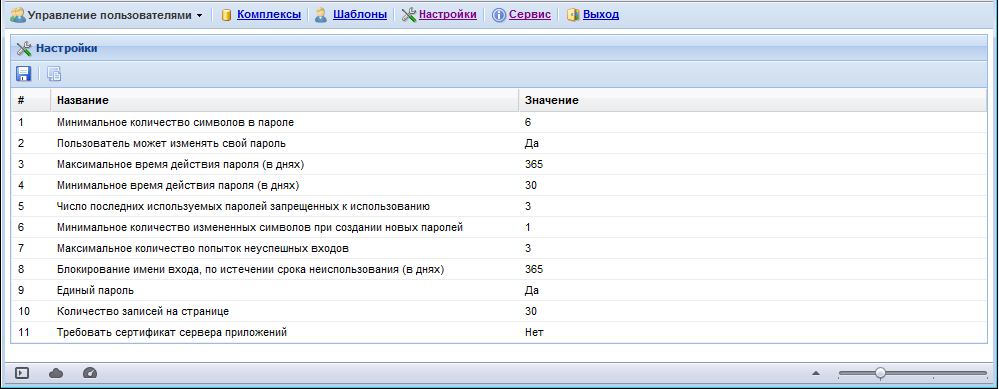
Шаблон будет сохранен в списке и доступен для назначения пользователям.

* + 1. Настройки

Выберите пункт «Настройки» главного меню.

Меню => Настройки

Открывшееся окно содержит список настроек политики паролей, которые учитываются при создании и редактировании учетных записей пользователей (Рисунок 21).



1. . Настройки политики паролей

Политика паролей определяется следующим набором настроек:

Минимальное количество символов в пароле – при использовании политики паролей нельзя будет установить пароль пользователя с меньшим количеством символов, чем указано в данной настройке.

Пользователь может изменять свой пароль – устанавливает возможность для пользователя изменить свой пароль в соответствующем режиме в ПК, но данный пароль будет действовать только при подключении через СА. Локальное изменение пароля (только для данной базы, при отключенном СА) возможно при незаполненном поле «Пароль БД» в окне редактирования пользователя в СА (Рисунок 9).

Максимальное время действия пароля (в днях) – количество дней, по истечении которых пользователь в обязательном порядке должен сменить свой пароль.

Минимальное время действия пароля (в днях) – срок, до истечения которого пользователь не может поменять свой пароль (если иное не установлено в приоритетной настройке «Сменить пароль при следующем входе» в окне регистрации пользователя (Рисунок 9).

Число последних используемых паролей, запрещенных к использованию – при изменении пароля пользователь не сможет вернуться к одному из старых паролей, если он входит в указанное в данной настройке количество предшествующих.

Минимальное количество измененных символов при создании новых паролей – при создании нового пароля путем изменения старого пользователю необходимо изменить в старом пароле не меньшее количество символов, чем указано в данной настройке. Например, при значении текущего пароля «123456», для нового пароля недопустимо значение «123457», если в настройке указано значение «2» (и более).

Максимальное количество попыток неуспешных входов – при вводе некорректного пароля указанное в данной настройке количество раз, учетная запись пользователя будет заблокирована во всех прикладных программных комплексах.

Блокирование имени входа, по истечении срока неиспользования (в днях) – в настройке указывается количество дней, через которое учетная запись пользователя будет заблокирована при условии, что ею не пользовались весь указанный период.

Единый пароль – для пользователей устанавливается единый (одинаковый) пароль для СА и всех прикладных ПК.

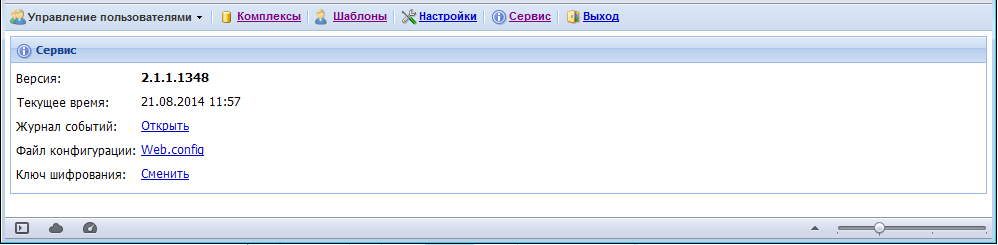
Количество записей на странице – количество выводимых строк при разбиении списка пользователей на страницы (относится к спискам СА).

Требовать сертификат сервера приложений – при установке значения «Да» подключение будет осуществляться при наличии допустимого сертификата сервера приложений.

* + 1. Сервис

Выберите пункт «Сервис» главного меню (Рисунок 22).

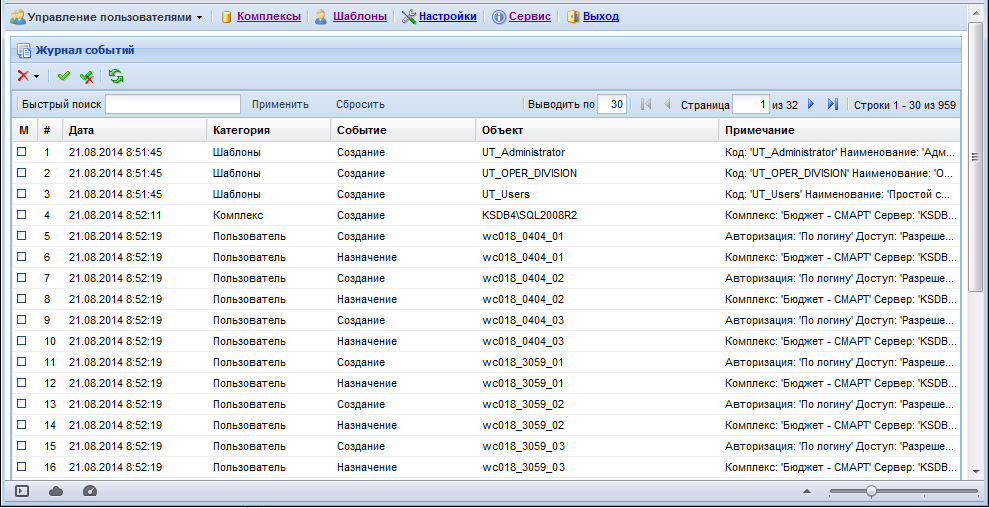
Меню => Сервис



1. . Меню «Сервис»

Окно «Сервис» содержит:

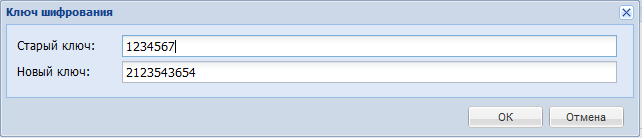
* сведения о версии СА на текущее время;
* ссылку Журнал событий: «Открыть» перехода на журнал событий (открывается в новой вкладке, Рисунок 23);



1. . Журнал событий

* ссылку Файл конфигурации: «Web.config», позволяющую открыть в новой вкладке для просмотра файл конфигурации;
* ссылку изменения ключа шифрования паролей в СА.

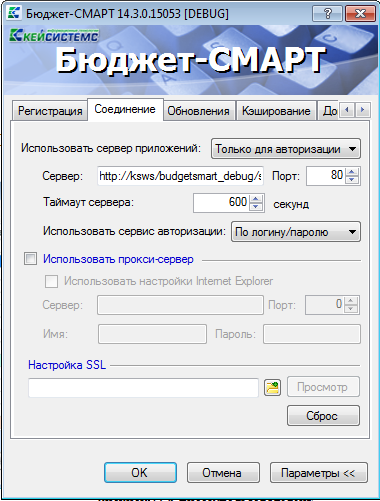
Ключ генерируется администратором при установке СА и прописывается в файле конфигурации СА. При подозрении на несанкционированное проникновение или при наличии других причин осуществляется изменение ключа шифрования: по ссылке «Сменить» откроется окно изменения, в котором необходимо ввести старый и новый ключ (Рисунок 24).



1. . Изменение ключа шифрования паролей в СА
   1. Подготовка ПК к работе через СА

Для входа и последующей работы в прикладном ПК пользователей, зарегистрированных через СА, необходимо выполнение в БД данного ПК следующих условий:

На вкладке «Соединение» окна регистрации ПК должен быть указан адрес размещения СА в поле Сервер. В настройке «Использовать сервер приложений» необходимо указать либо значение «Да» для работы через сервис приложений, либо значение «Только для авторизации» для работы в локальной сети (Рисунок 37).



1. . Вкладка «Соединение»

В ПК должен быть зарегистрирован виртуальный пользователь, являющийся системным администратором, который будет автором всех действий, выполненных над ПК через СА.

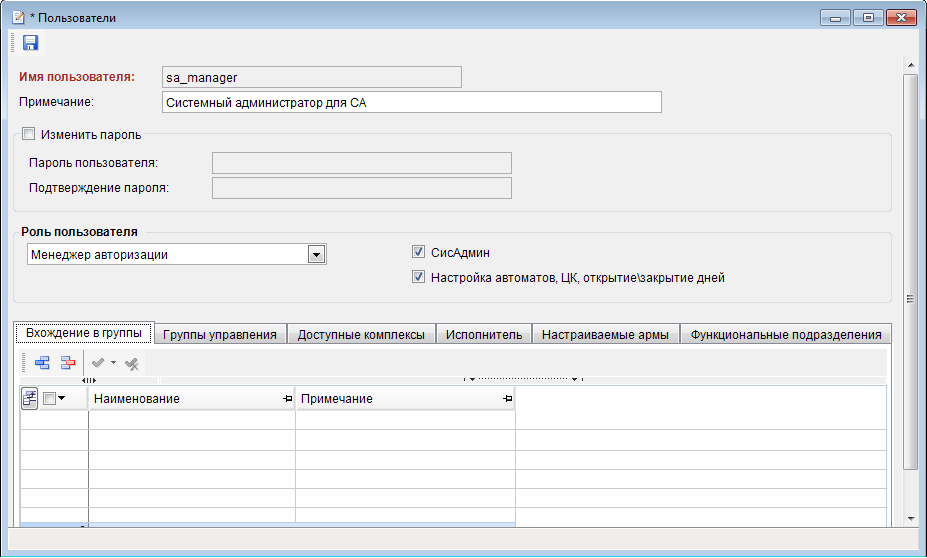
* + 1. Регистрация менеджера авторизации в прикладном ПК

Зарегистрируйте в базе ПК «Бюджет-СМАРТ» менеджера авторизации.

Войдите в БД ПК «Бюджет-СМАРТ» под учетной записью системного администратора. Выберите строку «Пользователи» в раскрывающемся списке пункта «Настройки» главного меню.

Главное меню => Настройки => Пользователи

Нажмите кнопку  Создать панели инструментов списка пользователей. Откроется окно добавления/редактирования учетной записи пользователя (Рисунок 26).



1. . Окно добавления/редактирования учетной записи пользователя

Для новой учетной записи заполните следующие поля:

* Имя пользователя – введите значение «sa\_manager»;

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | Возможно указание другого имени для системного администратора СА, но это имя должно быть прописано в файле конфигурации «Web.config» СА (см. Рисунок 22). |  |
|  |  |  |

* Примечание – введите значение «Системный администратор для СА»;
* Роль пользователя – выберите в раскрывающемся списке значение «Менеджер авторизации».

Установите флажки в поля СисАдмин и Настройка автоматов ЦК, открытие\закрытие дней.

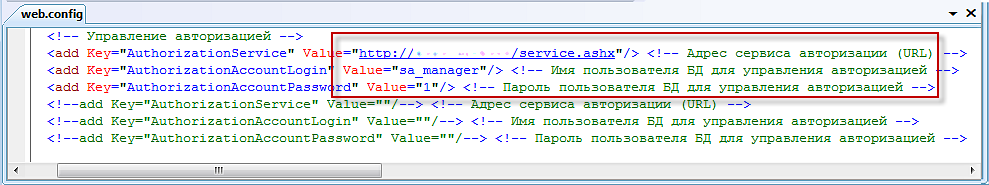
Сохраните данные новой учетной записи по кнопке  Сохранить.

* + 1. Редактирование файла «Web.config» прикладного ПК

В соответствии с созданной учетной записью менеджера авторизации необходимо внести изменения в файл «Web.config», в раздел «Управление авторизацией».

В данном файле необходимо указать следующие параметры:

* **Ошибка! Недопустимый объект гиперссылки.** - адрес сервиса авторизации;
* Имя пользователя БД для управления авторизацией;
* Пароль пользователя БД для управления авторизацией (Рисунок 27).



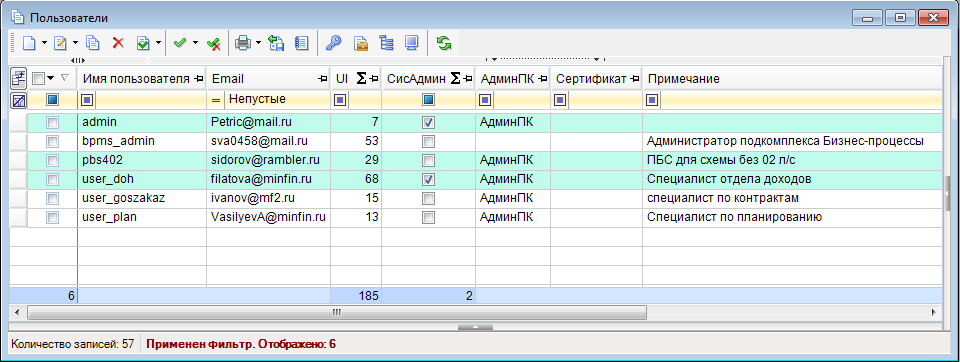
1. . Окно редактирования файла «Web.config»
   * 1. Работа со списком пользователей в прикладном ПК

Выберите строку «Пользователи» в раскрывающемся списке пункта «Настройки» главного меню.

Главное меню => Настройки => Пользователи

В открывшемся списке пользователей учетные записи, созданные в СА, выделены зеленым цветом (Рисунок 28).

Редактирование параметров такой учетной записи недоступно, т.к. оно осуществляется непосредственно на СА. Возможность изменения пароля определяется настройками политики паролей СА (п. 1.1.9).



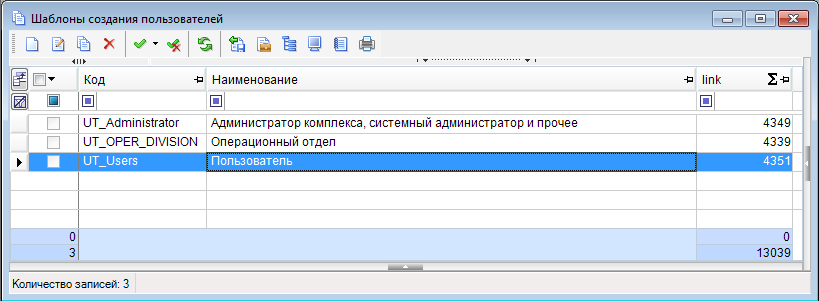
1. . Список пользователей

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | При передаче учетной записи пользователя в СА и последующем входе под данной учетной записью в ПК для нее применяются все правила учетных записей, созданных в СА: она выделяется зеленым цветом, реквизиты становятся недоступны для редактирования, возможность изменения пароля также определяется описанными в данном руководстве настройками СА (Рисунок 22). |  |
|  |  |  |

* + 1. Создание шаблона в прикладном ПК

Войдите в ПК «Бюджет-СМАРТ». В главном меню выберите пункт «Шаблоны создания пользователей» (Рисунок 29).

Главное меню => Настройки => Шаблоны создания пользователей



1. . Список шаблонов создания учетных записей пользователей в ПК «Бюджет-СМАРТ»

Для создания нового шаблона нажмите кнопку  Создать, для редактирования уже существующего шаблона нажмите кнопку  Редактировать. В окне добавления/редактирования (Рисунок 30) укажите следующие параметры шаблона:

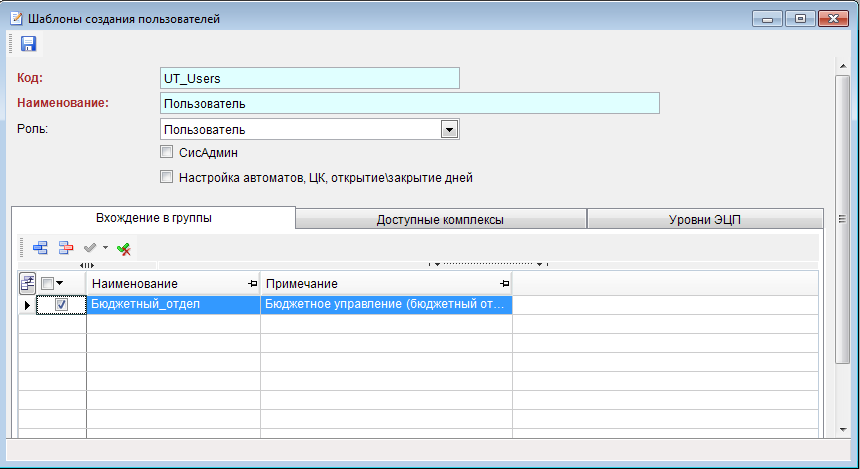
Код – код шаблона (в СА шаблон выбирается по коду);

Наименование – наименование шаблона;

Роль – выбирается из раскрывающегося списка («Пользователь» или «Администратор комплекса»);

СисАдмин – установка признака системного администратора для пользователей с данным шаблоном доступа;

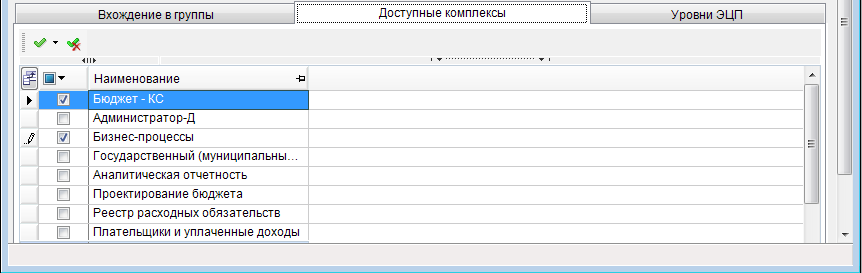
Настройка автоматов, ЦК, открытие\закрытие дней – данной настройкой определяется доступ к настройкам Центра контролей, автоматам (простановки операций, формирования первичного образа и пр.) ПК, открытие и закрытие дней.



1. . Окно создания шаблона в ПК «Бюджет-СМАРТ»

Далее необходимо включить пользователей, которым будет назначен данный шаблон, в одну или несколько групп ПК на вкладке «Вхождение в группы». Для добавления группы воспользуйтесь кнопкой  Добавить строку, затем выберите требуемое значение из списка доступных групп. Удаление из шаблона группы осуществляется по кнопке  Удалить строку.

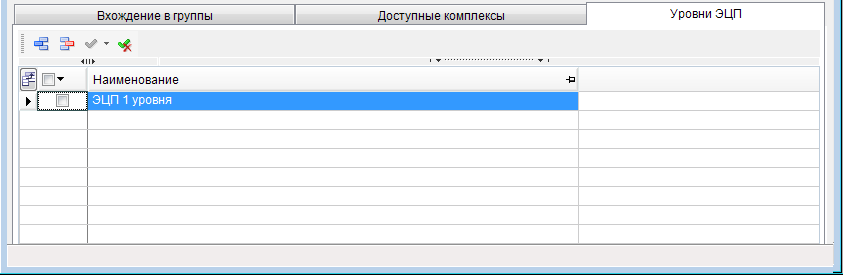
Назначение комплексов задач, находящихся в составе ПК «Бюджет-Смарт», которые будут доступны пользователям с данным шаблоном, осуществляется на вкладке «Доступные Комплексы» (Рисунок 31).



1. . Окно выбора доступных пользователям комплексов задач

Комплексы добавляются путем установки флажков в соответствующие поля списка, назначенный к ним доступ сохраняется при сохранении всего шаблона.

На вкладке «Уровни ЭЦП» доступно назначение в шаблоне доступных для использования уровней ЭП (Рисунок 32).



1. . Окно выбора доступных пользователям уровней ЭП

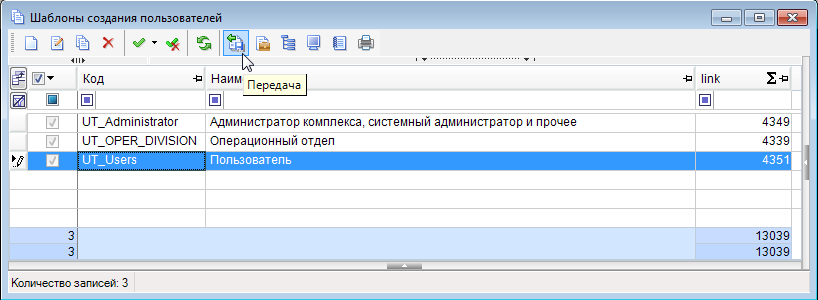
Для добавления уровня воспользуйтесь кнопкой  Добавить строку, затем выберите требуемое значение из списка доступных уровней. Удаление из шаблона уровня осуществляется по кнопке  Удалить строку.

Сохранение всех изменений шаблона прав доступа осуществляется по кнопке  Сохранить.

* + 1. Экспорт шаблона из прикладного ПК

Сохраненные шаблоны доступны для экспорта из ПК «Бюджет-СМАРТ» в режиме списка шаблонов (Рисунок 33).

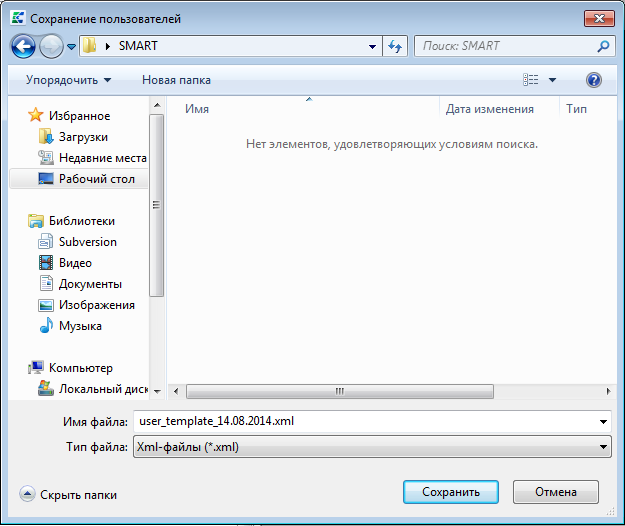
Главное меню => Настройки => Шаблоны создания пользователей



1. . Выбор шаблонов для передачи

Отметьте в списке шаблонов те, которые предназначены для экспорта и нажмите кнопку  Передача.

В открывшемся окне укажите каталог для сохранения файла выгрузки шаблонов в формате user\_template\_ДД.ММ.ГГГГ.xml и нажмите кнопку [Сохранить] (Рисунок 34).

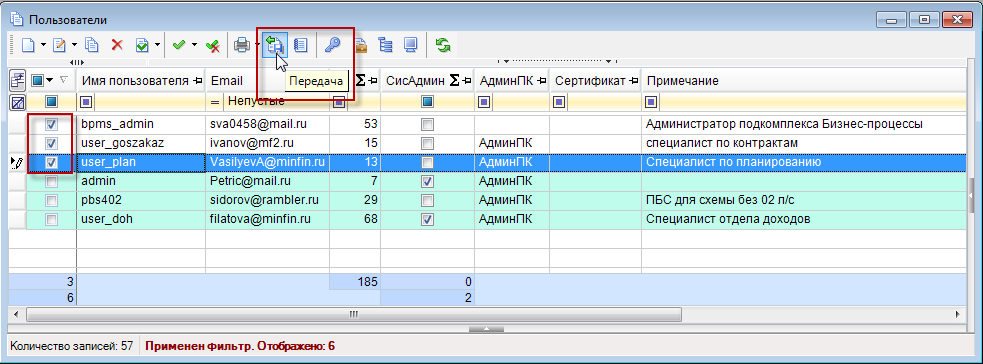


1. . Передача шаблонов

Выгруженный файл будет автоматически сохранен в указанном каталоге и доступен для импорта в СА в соответствии с описанием, приведенным в п. 1.1.8.1.

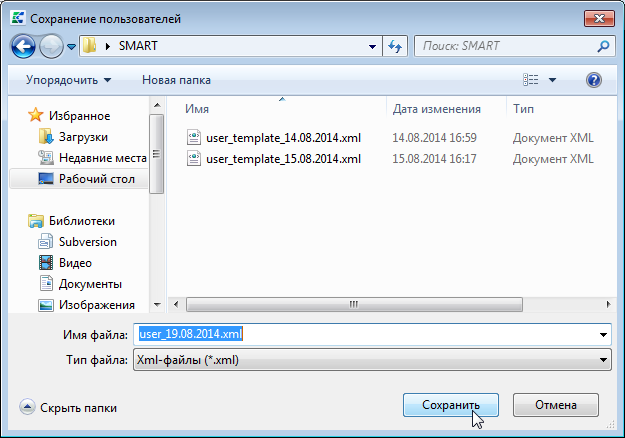
* + 1. Экспорт учетных записей пользователей

Для экспорта учетных записей пользователей отметьте данные записи в списке и нажмите кнопку  Передача (Рисунок 35).



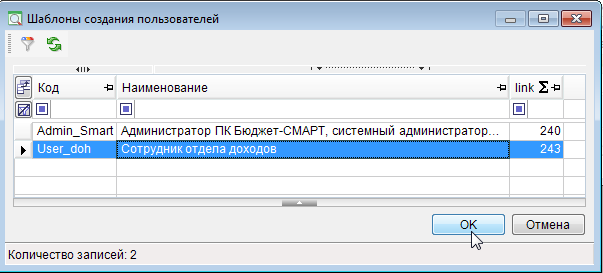
1. . Выбор учетных записей пользователей для передачи

Выберите каталог размещения файла user\_ДД.ММ.ГГГГ.xml на компьютере и нажмите кнопку [Сохранить] (Рисунок 36).



1. . Выбор каталога для размещения файла выгружаемых учетных записей

Далее будет предложено выбрать шаблон прав доступа, с которыми будут выгружены текущие учетные записи. Выберите шаблон и нажмите кнопку [ОК] (Рисунок 37).



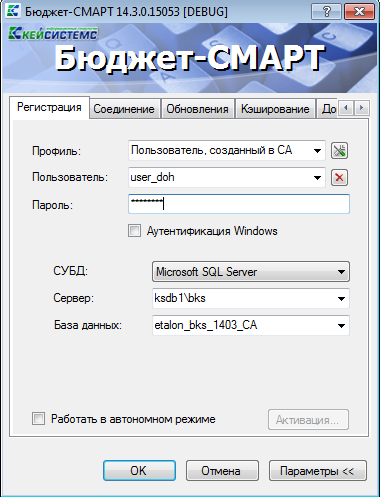
1. . Выбор шаблона прав доступа выгружаемых учетных записей

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  | При экспорте учетных записей пользователей указывается только один шаблон, который будет применен ко всем выбранным учетным записям. Поэтому не следует единовременно выгружать (в один файл) учетные записи пользователей, для которых требуется установить различные шаблоны создания учетных записей. |  |
|  |  |  |

Выгруженный файл будет автоматически сохранен в указанном каталоге и доступен для импорта в СА в соответствии с описанием, приведенным в п.1.1.3.

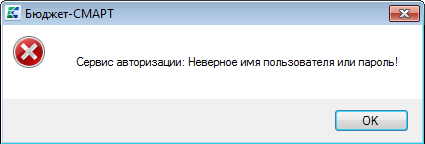
* 1. Работа в ПК через СА
     1. Вход в программный комплекс через СА

Вход в прикладной ПК для пользователя, зарегистрированного через СА, осуществляется стандартным способом: путем ввода параметров учетной записи в окне регистрации ПК (Рисунок 38).



1. . Вкладка «Регистрация»

При входе СА осуществляет проверку учетных данных в выбранной БД. При выявлении несоответствий вход блокируется с выводом соответствующего предупреждающего сообщения, которое начинается с указания СА как инициатора блокировки (Рисунок 39).



1. . Сообщение СА

При успешном прохождении проверки пользователь сможет приступить к работе с режимами в соответствии с назначенными ему правами доступа.

1. Рекомендации по освоению
   1. Настройка сертификатов

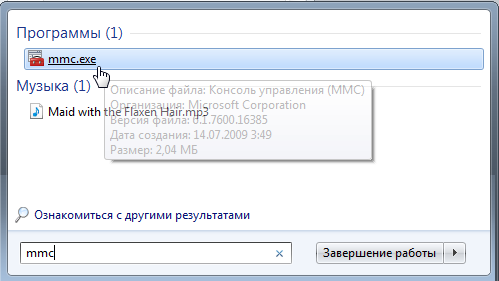
В случаях, когда сервис приложений и сервис авторизации расположены на разных серверах, существует возможность организации защищенного канала между ними.

Для этого понадобится 3 сертификата:

* Корневой сертификат;
* Сертификат сервера (сервиса авторизации);
* Сертификат клиента (сервера приложений).

Корневой сертификат необходимо установить в хранилище доверенных центров сертификатов на Сервисе авторизации. Для этого выполните следующие действия:

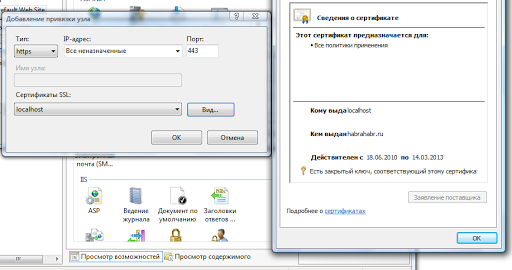
1. Запустите Консоль управления ММС (выполните в командной строке файл mmc.ехе) (Рисунок 40).



1. 40. Переход к консоли управления ММС
2. Добавьте оснастку «Сертификаты».
3. Откройте «Доверенные корневые центры сертификации» и выполните импорт корневого сертификата.

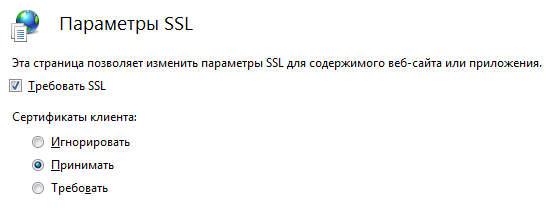
В консоли управления IIS на Сервисе авторизации откройте каталог «Сертификаты сервера», выберите опцию «Запрос установки сертификата» и укажите Сертификат сервера (Сервиса авторизации).

Далее в привязках для узла Сервиса авторизации создайте новую https - привязку и выберите из списка серверный сертификат (Рисунок 41).



1. 41. Добавление привязки узла

В настройках SSL для узла СА установите флажок в поле «Требовать SSL» и значение «Принимать» для настройки «Сертификаты клиента» (Рисунок 42).

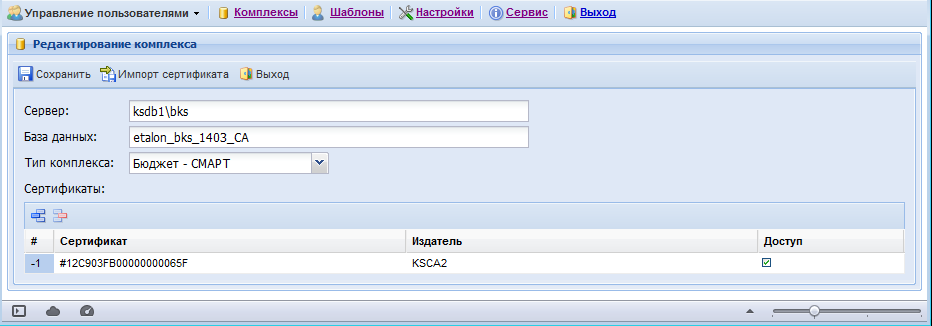


1. 42. Добавление привязки узла

На сервере приложений выполните импорт сертификата клиента в личное хранилище сертификатов.

В настройках Сервиса авторизации установите настройку «Требовать сертификат сервера приложений» в значение «Да».

В окне редактировании сведений о прикладном ПК в разделе «Сертификаты» пропишите требуемые сертификаты Сервера приложений (Рисунок 43). Для добавления сертификата используется процедура импорта (см. п. 1.1.7).



1. 43. Сведения о сертификате прикладного ПК на СА

Перечень сокращений

В документе используются следующие сокращения:

БД – База данных;

ПК – Программный комплекс;

СА – Сервис авторизации.

Лист регистрации изменений

|  |  |  |  |
| --- | --- | --- | --- |
| Номер версии | Примечание | Дата | ФИО исполнителя |
|
| 01 | Начальная версия | 11.09.2014 | Котова И.В. |