

Установка системы "iBank для Бизнеса" под Unix

Руководство администратора

Версия 2.7

Содержание

Общие сведения о системе "iBank для Бизнеса"	3
Системные требования	4
Перечень шагов по установке системы "iBank для Бизнеса"	6
Шаг 1. Разархивирование дистрибутива системы "iBank для Бизнеса"	7
Шаг 2. Настройка переменных окружения	12
Настройка Java	12
Настройка СКЗИ	12
Шаг 3. Создание объектов на сервере БД "iBank для Бизнеса"	13
Шаг 4. Загрузка справочника БИК и справочника БЭСП	14
Шаг 5. Загрузка справочника SWIFT	15
Шаг 6. Запуск инсталлятора системы	16
Шаг 7. Генерация SSL-сертификата	17
SSL-сертификат от Сертификационного Центра	17
Создание самозаверенного SSL-сертификата	19
Шаг 8. Конфигурирование сервера приложений "iBank для Бизнеса"	20
Запуск модуля "Конфигуратор системы для юридических лиц"	20
Установка Лицензии	22
Создание конфигурации сервера приложений	27
Настройка реквизитов банка и филиалов	39
Назначение главного администратора	42
Шаг 9. Запуск и остановка сервера приложений "iBank для Бизнеса"	44
Шаг 10. Формирование дистрибутивов клиентских модулей	45
Шаг 11. Формирование программы для подготовки рабочего места клиента	47
Шаг 12. Вход в модули системы	49
Шаг 13. Загрузка производственного календаря	51
Приложение 1. Настройка СКЗИ	53
Выбор типа криптографии, используемой на стороне сервера приложений	53
Выбор типов криптографии, используемых на стороне клиента	54
Установка СКЗИ "Крипто-КОМ 3.5" на стороне клиента/ сервера приложений	55
Приложение 2. Рекомендации по размещению компонент системы "iBank для Бизнеса"	56
Приложение 3. Рекомендации по техническому обеспечению	57
Приложение 4. Список логов сервера приложений	59
Приложение 5. Информация о совместимости и обновлении системы	60

Общие сведения о системе "iBank для Бизнеса"

Настоящий документ является инструкцией по установке системы для корпоративных клиентов "iBank для Бизнеса" под операционную систему Unix. Процесс установки поделен на отдельные шаги, каждый шаг подробно описан ниже.

Система "iBank для Бизнеса" (далее система) предназначена для продвижения и предоставления услуг электронного банкинга корпоративным клиентам.

Система устанавливается в банке и позволяет обслуживать корпоративных клиентов с использованием всех каналов доступа — Интернет, телефон, SMS, мобильные устройства и др.

Система позиционируется как единая платформа электронного банкинга и состоит из модулей для обслуживания корпоративных клиентов: Интернет-Банк, iBank для 1С, Мобильный Банк, SMS-Банк, Тикер, а также дополнительных сервисов: Центр финансового контроля (ЦФК), Корпоративное бюджетирование, Контроль расчетов по договорам, Корпоративный автоклиент, Банковский ассистент, Зарплатные проекты, Постоянные поручения.

Система относится к системам защищенного электронного документооборота. Обмен электронными документами происходит между банком и клиентом.

Для обеспечения аутентичности (доказательства авторства) и целостности документа используется механизм электронной подписи под электронными документами.

Именно электронный документ с электронной подписью клиента является основанием для совершения банком финансовых операций и доказательной базой при разрешении конфликтной ситуации.

В системе реализованы российские криптографические алгоритмы в соответствии с ГОСТ 28147-89 (шифрование, имитовставка), ГОСТ Р 34.11-2012 (хеш-функция) и ГОСТ Р 34.10-2012 (ЭП на эллиптических кривых).

Системные требования

Банковский сервер

Для работы сервера требуется любая СУБД из списка:

- Microsoft SQL Server (2012, 2014, 2016 (SP2), 2017, 2019);
- Oracle (10g, 11g, 12c, 19c);
- PostgreSQL (9.0 и выше).

Сервер приложений может потребовать до 1,5 ГБ виртуальной памяти. По умолчанию сервер сконфигурирован на использование большого числа сервисов обслуживания клиентов. Вы можете изменить объем доступной памяти в настройках хоста в модуле "Конфигуратор системы для юридических лиц" (параметр "Xmx").

Операционная система

Работа приложений клиентов и банковских сотрудников обеспечена на ОС:

- Microsoft Windows: 7 (x86/x64), 8 (x86/x64), 8.1 (x86/x64), 10 (x86/x64) и выше;
- Ubuntu и прочие deb-дистрибутивы (последние версии x64);
- Apple Mac OS X: 10.7 и выше;
- Astra Linux;
- Требования к ОС для мобильных устройств:
 - iOS (версия 14.0 и выше);
 - Android (версия 7.0 и выше).

Java

Среда исполнения для приложений клиентов, банковских сотрудников и сервера приложений:

- Java 8 и выше;
- Liberica JDK.

Рекомендуется включать автоматическое обновление и использовать последнюю версию Java.

Рабочее место корпоративного клиента и банковского операциониста

Web-браузер (Microsoft Edge; Google Chrome; Яндекс Браузер; Firefox; Opera; Atom; Safari) + BIFIT Signer Host для использования электронной подписи.

Рекомендуется включать автоматическое обновление и использовать последние версии браузеров.

Конфигуратор системы для юридических лиц

Java 8 и выше.

Администратор банка/филиала

Java 8 и выше.

До версии системы 2023.5 был доступен единственный способ эксплуатации модуля — web-браузер с поддержкой Java (Internet Explorer версия 11, Safari версия 9 и выше) + Java 8 (32-bit) и выше.

Программные СКЗИ

Для криптографической защиты информации встроена поддержка многоплатформенной криптобиблиотеки СКЗИ Крипто-КОМ 3.5. компании Сигнал-КОМ.

Аппаратные СКЗИ

Для безопасного хранения и использования ключей электронной подписи встроена поддержка USB-токенов, сертифицированных ФСБ России:

- MS_KEY K – Ангара,
- Рутокен ЭЦП 2.0;
- Рутокен ЭЦП 2.0 2100;
- Рутокен ЭЦП 2.0 3000;
- Рутокен ЭЦП 3.0;
- Рутокен ЭЦП 3.0 3220.

Драйвера для USB-токенов

В последних версиях ОС не требуется установка драйверов для USB-токенов.

Рекомендации по настройке СКЗИ см. в разделе [Приложение 1](#).

Рекомендации по размещению компонентов системы "iBank для Бизнеса" см. в разделе [Приложение 2](#).

Рекомендации по техническому обеспечению см. в разделе [Приложение 3](#).

Перечень шагов по установке системы "iBank для Бизнеса"

1. Разархивирование дистрибутива системы (см. [Шаг 1](#));
2. Подготовка к запуску инсталлятора системы:
 - настройка Java и СКЗИ (см. [Шаг 2](#));
 - настройка создания базы данных системы "iBank для Бизнеса" (см. [Шаг 3](#));
 - настройка загрузки справочника БИК и справочника БЭСП (см. [Шаг 4](#));
 - настройка загрузки справочника SWIFT (см. [Шаг 5](#));
3. Запуск инсталлятора системы (см. [Шаг 6](#));
4. Генерация SSL-сертификата (см. [Шаг 7](#));
5. Установка Лицензии и конфигурирование сервера приложений "iBank для Бизнеса" (см. [Шаг 8](#));
6. Запуск сервера приложений (см. [Шаг 9](#));
7. Формирование дистрибутивов клиентских модулей и программы для подготовки рабочего места клиента (см. [Шаг 10](#) – [Шаг 11](#));
8. Проверка доступности модулей системы для клиентов банка и банковских сотрудников (см. [Шаг 12](#));
9. Загрузка производственного календаря (см. [Шаг 13](#)).

Шаг 1. Разархивирование дистрибутива системы "iBank для Бизнеса"

Примечание:

Поскольку в систему "iBank для Бизнеса" встроен механизм управления Лицензиями с привязкой к БИК банка, то перед установкой и настройкой системы необходимо связаться с сотрудниками компании "БИФИТ" по тел.: 8-495-532-15-02, 8-499-705-01-01, 8-800-333-911-0 или по электронной почте support@bifit.com и получить файл с Лицензией на необходимую конфигурацию банковской компоненты и необходимое количество клиентов.

Для проведения опытной эксплуатации Лицензия на один банк и 5 — 10 клиентов-юридических лиц предоставляется бесплатно.

Получите дистрибутив системы — `iBankCorporate-XXXX.X.XX.zip`. Скопируйте и распакуйте архив в одноименный каталог, например, `/usr/local/iBankCorporate`

В результате разархивирования будет создана следующая структура подкаталогов:

Каталог	Содержимое
<code>doc</code>	Руководства по установке системы "iBank для Бизнеса" под Windows, Unix
<code>modules</code>	Архивы с компонентами системы "iBank для Бизнеса"
Файл <code>version</code> содержит номер версии системы	

Содержимое каталога `modules` состоит из:

Файл	Содержимое
<code>balance-confirmation-util.zip</code>	Архив с ресурсами утилиты, предназначенной для создания документов "Подтверждение остатков"
<code>mobile_lite_demo_creator.zip</code>	Архив с ресурсами утилиты, предназначенной для создания демонстрационной учетной записи для модуля "Мобильный Банк для микробизнеса"
<code>pegasus_channel.zip</code>	Архив с ресурсами модуля "Шлюз рассылки уведомлений сервиса SMS-Банк"
<code>server.zip</code>	Архив с ресурсами сервера приложений системы "iBank для Бизнеса"
<code>sign-opers.zip</code>	Архив с ресурсами утилиты банковского сотрудника, предназначенной для формирования ЭП под выпиской клиента
<code>syscon.zip</code>	Архив с ресурсами модуля "Конфигуратор системы для юридических лиц"

Распакуйте архивы `server.zip` и `syscon.zip` каталога `modules` в отдельные каталоги, например, в `/usr/local/iBankCorporate/server` и `/usr/local/iBankCorporate/syscon` соответственно.

Использование нескольких (дополнительных) серверов приложений и/или нескольких модулей "Конфигуратор системы для юридических лиц" требует отдельной установки и настройки этих приложений (подробнее см. в соответствующих разделах руководства).

В результате разархивирования `syscon.zip` будет создана следующая структура подкаталогов:

Каталог	Содержимое
bin	<p>Командные скрипты для выполнения следующих действий:</p> <ul style="list-style-type: none"> — запуск модуля "Конфигуратор системы для юридических лиц" (<code>syscon.(bat sh)</code>)*; — настройка переменных для выполнения различных скриптов (<code>setvars.(bat sh).sample</code>); — служебный файл для выполнения различных скриптов (<code>setenv.(bat sh)</code>); — установка системы "iBank для Бизнеса" (<code>install.(bat sh)</code>)*; — формирование БД системы "iBank для Бизнеса", а также генерация скриптов создания БД (<code>dbcreator.(bat sh)</code>)*; — загрузка справочника российских банков по 595-П в БД (<code>load_bic_595p.(bat sh)</code>)*; — загрузка справочника телефонных номеров операторов сотовой связи (def-кодов) в БД (<code>load_def_codes.(bat sh)</code>)*; — загрузка справочника ФИАС в БД (<code>load_fias.(bat sh)</code>)*; — загрузка курсов валют ЦБ РФ в формате XML (<code>load_CBRrates.(bat sh)</code>)*; — загрузка справочника стран в БД (<code>load_countries.(bat sh)</code>)*; — загрузка справочника таможенных органов в БД (<code>load_customs_institution.(bat sh)</code>)*; — загрузка справочника КБК в БД (<code>load_kbk.(bat sh)</code>)*; — загрузка справочника SWIFT в БД (<code>load_swift_BICDIR2018_BICPLUS.(bat sh)</code>)*; — загрузка налогового календаря в БД (<code>load_tax_calendar.(bat sh)</code>)*; — загрузка значений масок счетов получателей бюджетных платежей" (<code>load_accounts.(bat sh)</code>)*; — загрузка XML-файла данных для OTP-токенов в БД (<code>load_tokens.(bat sh)</code>)**; — синхронизация OTP-токенов (ActivIdentity Mini Token AT, Vasco DIGIPASS GO 3) с сервером приложений системы "iBank для Бизнеса" (<code>sync_token.(bat sh)</code>)**; — загрузка ресурсов в БД (<code>load_res.(bat sh)</code>)**; — загрузка календаря праздничных дней и рабочих дней, приходящихся на выходные, в БД (<code>load_holidays_calendar.(bat sh)</code>)*; — загрузка детализированного календаря налоговых событий в БД (<code>load_detailed_tax_calendar.(bat sh)</code>)*; — загрузка классификатора адресов в формате ГАР в БД (<code>load_gar.(bat sh)</code>)*; — загрузка справочника МСС (категории продавца) в БД (<code>load_mcc.(bat sh)</code>)* — загрузка справочника казначейских счетов в БД (<code>load_treasury_accounts.(bat sh)</code>)*
conf	Конфигурационные файлы модуля "Конфигуратор системы для юридических лиц"

firmware	Ресурсы системы, которые загружаются в БД системы "iBank для Бизнеса": прошивка Интернет-Банка (firmware); xslt-шаблоны SMS-Банка; шаблоны выгрузки документов в Excel (xls-templates);
lib	Библиотечные файлы модуля "Конфигуратор системы для юридических лиц"
logs	Каталог для сохранения журналов (логов) работы модуля "Конфигуратор системы для юридических лиц", журналов формирования БД системы, журналов загрузки ресурсов системы, журналов загрузки справочников БИК, SWIFT
refs	Подкаталоги, из которых загружаются справочники, используемые в системе "iBank для Бизнеса" (БИК, SWIFT, КБК, ФИАС, справочник стран, справочник курсов валют, производственный календарь)
templates	Шаблоны конфигурационных файлов системы "iBank для Бизнеса"

* запуск выполняется из командной консоли ОС

** запуск возможен как из графического интерфейса модуля "Конфигуратор системы для юридических лиц", так и из командной консоли ОС

В результате разархивирования `server.zip` будет создана следующая структура подкаталогов:

Каталог	Содержимое
bin	Командные скрипты для выполнения следующих действий: — загрузка конфигурации хоста и запуск сервера приложений "iBank для Бизнеса"; — выявление входа в систему клиентов из запрещенных регионов на основе лог-файлов доступа и блокирование их ключей; — заполнение таблицы IP-фильтра на основании парсинга лог-файлов; — формирование клиентских дистрибутивов системы "iBank для Бизнеса".
conf	Конфигурационные файлы сервера приложений "iBank для Бизнеса"
lib	Библиотечные файлы сервера приложений "iBank для Бизнеса"
logs	Журналы (логи) работы сервера приложений "iBank для Бизнеса" и серверных модулей системы "iBank для Бизнеса"
temp	Временные файлы
webapps-local	Части серверных модулей системы "iBank для Бизнеса" и корневой каталог ROOT встроенного web-сервера для работы сотрудников банка
webapps-public	Части серверных модулей системы "iBank для Бизнеса" и корневой каталог ROOT встроенного web-сервера для работы клиентов банка
work	Системный каталог сервера приложений
Файл <code>ReleaseNotes.pdf</code> содержит краткое описание изменений текущей версии системы	

В данном руководстве приняты обозначения:

`$SYSICON_ROOT` — каталог с установленным модулем "Конфигуратор системы для юридических лиц".

`$SERVER_HOME` — каталог с установленным сервером приложений системы "iBank для Бизнеса".

Актуальная документация по системе "iBank для Бизнеса" для клиентов и банковских сотрудников включена в дистрибутив и находится в каталогах: для клиентов — `$SERVER_ROOT/webapps-public/ROOT/docs`, для банковских сотрудников — `$SERVER_ROOT/webapps-local/ROOT/docs`

По умолчанию документация доступна клиентам по ссылке [Документация](#) на странице входа (см. [рис. 1](#)).

Список **Документация** настраивается в модуле "Система управления контентом (CMS)" в разделе **Настройка страницы входа**, ссылка **Содержимое нижнего всплывающего окна страницы входа**.

Для банковских сотрудников — по ссылке **Документация** на странице входа или по адресу `https://<адрес сервера приложений>:9443/docs` Список настраивается — `$SERVER_ROOT/webapps-local/ROOT/docs/index.html`

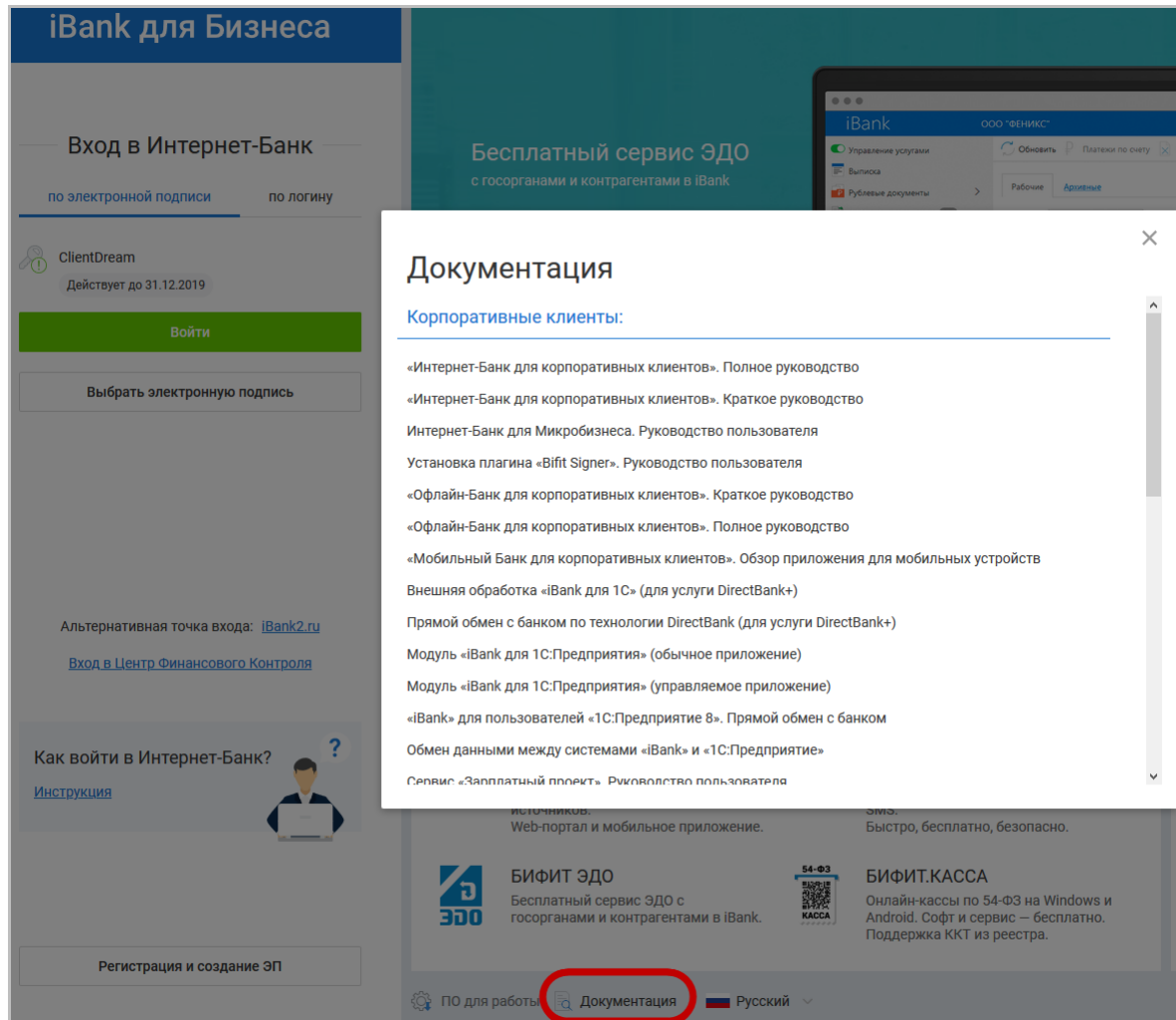


Рис. 1. Список документации для клиентов

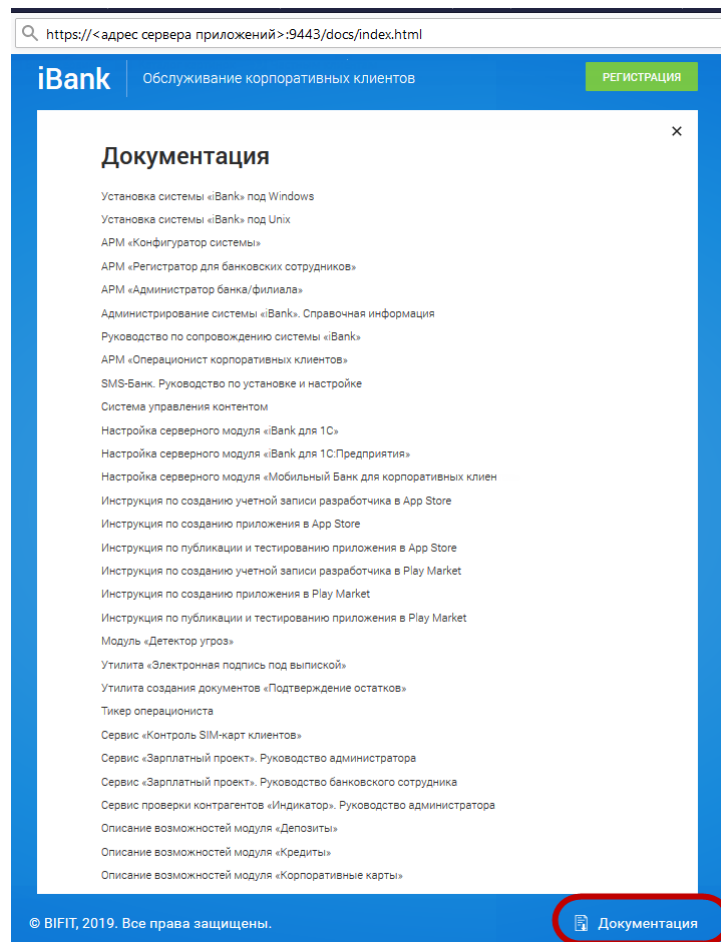


Рис. 2. Список документации для сотрудников банка

Шаг 2. Настройка переменных окружения

Переменные окружения задаются в файле %SYSCON_ROOT%/bin/setvars.sh. В составе дистрибутива находится файл %SYSCON_ROOT%/bin/setvars.sh.sample, для которого необходимо удалить расширение sample и выполнить настройку переменных окружения.

Настройка Java

Компоненты системы "iBank для Бизнеса" реализованы на Java, поэтому на компьютере, где происходит работа с ними, необходимо наличие работоспособной Java. Дистрибутив последней версии для используемой ОС вы можете получить с сайта разработчика — <http://www.java.com/ru>

Для настройки Java необходимо выполнить:

- В случае использования для Java системных переменных окружения в их значениях необходимо указывать путь к каталогу с установленной Java в переменной JAVA_HOME, например, /usr/local/java/jdk1.8.0_51
- Если вы **не** используете для Java системных переменных, то необходимо выполнить индивидуальную настройку приложений системы "iBank для Бизнеса" (см. разделы [Индивидуальная настройка Java для модуля "Конфигуратор системы"](#) для юридических лиц, [Индивидуальная настройка Java для сервера приложений](#)).

Для проверки наличия и версии Java, установленной на сервере используйте команду:

```
java -version
```

Установленную версию Java необходимо использовать без установки дополнительных библиотек для СКЗИ "КриптоПро" — xmlsec-1.5.0.jar, log4j-1.2.17.jar, commons-logging-1.1.1.jar

Настройка СКЗИ

Для обеспечения защиты конфиденциальной информации на стороне сервера приложений системы "iBank для Бизнеса" необходимо наличие средств криптографической защиты информации. СКЗИ используется для реализации функций формирования ключей шифрования и электронной подписи, выработки и проверки электронной подписи, шифрования и имитозащиты информации.

Для криптографической защиты информации в систему "iBank для Бизнеса" встроена поддержка сертифицированной ФСБ РФ многоплатформенной криптобиблиотеки СКЗИ "Крипто-КОМ 3.5" компании "Сигнал-КОМ".

Для ОС Linux криптобиблиотека представлена в виде динамических библиотек ("*.so"). Механизм ее использования встроены в клиентские и серверные приложения.

Криптобиблиотека предназначена для обеспечения защиты конфиденциальной информации, которая не является государственной тайной, от угроз нарушения конфиденциальности и целостности при помощи использования криптографических процедур, встроенных в прикладные программы.

Для получения файлов криптобиблиотеки обратитесь в компанию "БИФИТ".

Установка СКЗИ "Крипто-КОМ 3.5"

Выбор типа криптографии, используемой на стороне сервера приложений и клиента банка, а также установка СКЗИ "Крипто-КОМ 3.5" рассмотрены в разделе [Приложение 1](#).

Шаг 3. Создание объектов на сервере БД "iBank для Бизнеса"

По умолчанию база данных системы "iBank для Бизнеса" может быть создана во время установки системы. При запуске инсталлятора системы выполняется проверка на наличие БД на сервере СУБД согласно параметрам конфигурационного файла `$SYSCON_ROOT/conf/dbcreator.xml`. Если такая БД не будет найдена, то она будет создана, в противном случае это действие будет пропущено.

Для указания параметров создаваемой БД системы "iBank для Бизнеса" отредактируйте конфигурационный файл `dbcreator.xml`:

- `type` — Тип используемой СУБД. Допустимые значения: MSSQL, ORACLE, POSTGRESQL.
- `address` — Адрес для подключения к СУБД, задается в формате `host:port`, для ORACLE — `host:port:sid`.
- `name` — Имя БД системы "iBank для Бизнеса". Для ORACLE — часть имени табличных пространств.
- `storespace type="data" filename` — Путь до файла БД.
Для MSSQL, ORACLE путь указывается до файла, для POSTGRESQL — до каталога, в котором будут располагаться файлы БД. Каталог должен существовать и у него должны быть назначены полные права для администратора СУБД.
- `storespace type="temp" filename` — Путь до журнала транзакций для MSSQL, путь до файла временных данных для ORACLE. Для POSTGRESQL параметр игнорируется.
- `owner name password` — Логин и пароль владельца объектов создаваемой БД системы "iBank для Бизнеса".

Пример заполнения файла `dbcreator.xml` для СУБД MSSQL:

```
<Database>
  <type>MSSQL</type>
  <address>192.168.0.1:1433</address>
  <name>ibank</name>
  <storespace type="data" filename="C:\Program Files\Microsoft SQL Server
\MSSQL\Data\ibank.mdf"/>
  <storespace type="temp" filename="C:\Program Files\Microsoft SQL Server
\MSSQL\Data\ibank_temp.ldf"/>
  <owner name="ibank" password="change_on_install"/>
</Database>
```

Пример заполнения файла `dbcreator.xml` для СУБД ORACLE:

```
<Database>
  <type>ORACLE</type>
  <address>192.168.0.1:1433:ibank</address>
  <name>ibank</name>
  <storespace type="data" filename="/oradata/ibank/ibank.dbf"/>
  <storespace type="temp" filename="/oradata/ibank/ibank_temp.ldf"/>
  <owner name="ibank" password="change_on_install"/>
</Database>
```

После окончания работы инсталлятора (см. [Шаг 6](#)) в каталоге `$SYSCON_ROOT/conf` будет сформирован файл `connection.xml`, содержащий данные соединения с БД системы "iBank для Бизнеса".

Примечание:

Для БД рекомендуется использовать кодировку `cp1251/windows-1251` или совместимую с ней.

Шаг 4. Загрузка справочника БИК и справочника БЭСП

Сведения справочников БИК и БЭСП обновляются на основании информации, рассылаемой Банком России. В составе системы "iBank для Бизнеса" поставляется утилита для импорта справочника БИК из файлов 20210219_ED807_full.XML и TNP.DBF и справочника БЭСП из файлов с информацией об участниках расчетов системы БЭСП.

Утилита предназначена для первоначального импорта справочников и для выполнения их последующих обновлений. Импорт и обновление можно выполнять как для обоих справочников одновременно, так и по отдельности.

Примечание:

На этапе установки системы "iBank для Бизнеса" импорт справочника БИК является обязательным и выполняется в процессе работы инсталлятора системы.

Перед загрузкой справочников (запуском инсталлятора системы, отдельным запуском утилиты `$SYSCON_ROOT/bin/load_bic_595p.sh`) необходимо получить их последние версии и выполнить настройки:

- файлы 20210219_ED807_full.XML, TNP.DBF, а также файлы с информацией об участниках расчетов системы БЭСП поместите в каталог `$SYSCON_ROOT/refs/bic`

Для загрузки справочников из другого каталога в командном файле `$SYSCON_ROOT/bin/setvars.sh` укажите путь к требуемому каталогу с файлами справочников, отредактировав строку `set REFS_BIC_DIR=`

- при загрузке справочника БИК по умолчанию включена автозамена символа "№" на символ "N".

За замену символа "№" на символ "N" отвечает параметр `needReplaceNumberSymbol` исполняемого файла `$SYSCON_ROOT/bin/setvars.sh`. Параметр может принимать значения:

`true` — при загрузке справочника выполняется замена символа "№" на символ "N";

`false` — при загрузке справочника загружается символ "№".

При установке параметра в значение `false` необходимо установить значение свойства `documents.extended_chars.enable` (признак возможности указания в рублевых документах символов Ё, ё, №) в значение `true`. Это необходимо во избежание возникновения ошибок при работе системы со справочником БИК, содержащим символ "№".

Результат загрузки справочников в БД системы "iBank для Бизнеса" сохраняется в файл `$SYSCON_ROOT/logs/bic-595p.log`

Если загрузка справочников БИК, участников БЭСП не проходит, проверьте параметры:

- наличие доступа к серверу БД;
- наличие прав пользователя сервера БД;
- параметры конфигурационного файла `$SYSCON_ROOT/conf/connection.xml`
- наличие файлов справочника БИК: 20210219_ED807_full.XML и TNP.DBF и файлов для загрузки информации об участниках расчетов системы БЭСП;
- путь к каталогу с dbf-файлами справочника БИК и файлами справочника БЭСП в исполняемом файле `$SYSCON_ROOT/bin/setvars.sh`

Шаг 5. Загрузка справочника SWIFT

Этот шаг не является обязательным в процессе установки системы "iBank для Бизнеса".

В системе "iBank для Бизнеса" может использоваться справочник участников международной межбанковской системы передачи информации и совершения платежей (далее справочник SWIFT).

В составе системы поставляется утилита для импорта справочника SWIFT из файлов различных форматов, например, таких как `ct.dat`, `cu.dat`, `fi.dat`, `hd.dat`, `md5.sum`, `bicduam.dos`, `bicduct.dos`, `bicducu.dos`, `bicdufi.dos`, `bicduhd.dos`

Утилита предназначена для первоначального импорта справочника и для выполнения его последующих обновлений.

Примечание:

На этапе установки системы "iBank для Бизнеса" импорт справочника SWIFT может быть осуществлен в процессе работы инсталлятора системы.

Перед загрузкой справочника (запуском инсталлятора системы, отдельным запуском утилиты `$SYSCON_ROOT/bin/load_swift_BICDIR2018_BICPLUS.sh`) необходимо получить его последнюю версию и выполнить настройки:

- поместите в каталог `$SYSCON_ROOT/refs/swift` файлы последней версии справочника SWIFT;
Для загрузки справочников из другого каталога в исполняемом файле `$SYSCON_ROOT/bin/setvars.sh` укажите путь к каталогу с файлами справочника SWIFT, отредактировав строку `set REFS_SWIFT_DIR=`

Результат загрузки справочника в БД системы "iBank для Бизнеса" сохраняется в файл `$SYSCON_ROOT/logs/swift.log`

Если загрузка справочника SWIFT не проходит, проверьте параметры:

- наличие доступа к серверу БД;
- наличие прав пользователя сервера БД;
- параметры конфигурационного файла `$SYSCON_ROOT/conf/connection.xml`
- наличие файлов справочника SWIFT (описание формата файлов справочника см. выше);
- путь к каталогу с файлами справочника SWIFT в исполняемом файле `$SYSCON_ROOT/bin/setvars.sh`

Шаг 6. Запуск инсталлятора системы

Перед запуском инсталлятора проверьте:

1. настройки Java;
2. настройки подключения к БД системы "iBank для Бизнеса" в конфигурационном файле `$_SYSCON_ROOT/conf/dbcreator.xml`
3. наличие в каталоге `$_SYSCON_ROOT/refs` соответствующих подкаталогов с файлами справочников: БИК (обязательно), БЭСП, SWIFT

Запустите утилиту `$_SYSCON_ROOT/bin/install.sh`. После запуска инсталлятора будут выполнены задачи:

- Подготовка схемы данных системы "iBank для Бизнеса";
- Загрузка файла конфигурации;
- Создание БД системы "iBank для Бизнеса" (при необходимости);

Для подтверждения создания БД необходимо ввести имя пользователя с правами системного администратора СУБД и его пароль.

- Создание файла с параметрами подключения к БД системы "iBank для Бизнеса" — `$_SYSCON_ROOT/conf/connection.xml`;

Перед первым запуском сервера приложений необходимо скопировать файл `connection.xml` в каталог с установленным сервером приложений "iBank для Бизнеса" — `$_SERVER_ROOT/conf`.

- Загрузка справочников: БИК, БЭСП, SWIFT;
- Загрузка в БД системы "iBank для Бизнеса" ресурсов: прошивка Интернет-Банка; xslt-шаблоны SMS-Банка; шаблоны выгрузки документов в Excel.

Результат работы инсталлятора по каждой задаче будет сохранен в отдельный лог-файл в каталог `$_SYSCON_ROOT/logs`.

В случае появления в нем сообщений об ошибках свяжитесь со службой технической поддержки компании "БИФИТ" по телефону 8-495-532-15-02, 8-499-705-01-01, 8-800-333-911-0 или по электронной почте support@bifit.com

Далее необходимо выполнить конфигурирование сервера приложений в модуле "Конфигуратор системы для юридических лиц" (см. следующие разделы документа).

Шаг 7. Генерация SSL-сертификата

В системе "iBank для Бизнеса" в рамках сервера приложений "iBank для Бизнеса" работает вспомогательный web-сервер с поддержкой протокола SSL, который используется для безопасной работы с web-приложениями.

Для работы вспомогательного web-сервера необходим SSL-сертификат. При промышленной эксплуатации системы "iBank для Бизнеса" сертификат должен быть получен банком в одном из мировых Сертификационных Центров:

- VeriSign — <https://www.verisign.com>
- Thawte — <https://www.thawte.com>
- Хостинг Центр РБК (Российский дилер Thawte) — <http://www.ssl.ru>

Срок действия сертификата, как правило, составляет один год.

При опытной эксплуатации допустимо использование самозаверенного сертификата (сертификат, который банк выдает самому себе) с обязательной передачей клиентам на электронных носителях самозаверенного сертификата и последующей установкой сертификата в web-браузеры клиентов.

Важным вопросом является выбор домена, для которого будет получен сертификат. Как правило, банки выбирают домен `ibank.bankname.ru`. Вопрос выбора домена должен быть согласован с общей политикой продвижения услуг электронного банкинга.

SSL-сертификат от Сертификационного Центра

Процесс генерации SSL-сертификата состоит из:

1. создание хранилища секретных ключей и сертификатов;
2. генерация и отправка в Сертификационный Центр запроса на получение SSL-сертификата;
3. импорт полученного SSL-сертификата в хранилище.

Создание хранилища секретных ключей и сертификатов

Создание хранилища выполняется с помощью утилиты `keytool.exe`, входящей в состав дистрибутива Java.

Для создания хранилища запустите утилиту `keytool` с параметрами:

```
$JAVA_HOME/bin/keytool -genkey -alias ibank -keyalg RSA -sigalg SHA256withRSA
-keysize 2048 -keystore $SERVER_ROOT/conf/.sslkeystore -validity 730
```

где

`{-alias ibank}` — псевдоним (имя), под которым ваш сертификат будет помещен в хранилище и по которому вы впоследствии будете к нему обращаться. В данном примере — `ibank для Бизнеса`;

`{-keyalg RSA}` — тип алгоритма шифрования вашей подписи. В данном примере — `RSA`;

`{-sigalg SHA256withRSA}` — тип алгоритма, который будет использоваться для подписания сертификата. В данном примере — `SHA256withRSA`;

`{-keysize 2048}` — длина ключа шифрования. В данном примере — `2048` бит;

`{-keystore $SERVER_ROOT/conf/.sslkeystore}` — файл, в который следует поместить SSL-хранилище, после его создания В данном примере — `$SERVER_ROOT/conf/.sslkeystore`;

`{-validity 730}` — срок годности вашего сертификата. В данном примере — `730` дней (2 года).

В процессе работы утилита попросит вас указать имя домена, для которого требуется выдать сертификат, и его организацию-владельца. Информация запрашивается в виде последовательных вопросов и выглядит следующим образом:

```
Enter keystore password: <Введите пароль для доступа к новому хранилищу ключей>
(пароль должен быть не менее 7 символов и содержать как цифры, так и буквы)
```

```
What is your first and last name?
[Unknown]: ibank.bankname.ru
```

```
What is the name of your organizational unit?
[Unknown]: IT Department
```

```
What is the name of your organization?
[Unknown]: Bankname
```

```
What is the name of your City or Locality?
[Unknown]: Moscow
```

```
What is the name of your State or Province?
[Unknown]: Russia
```

```
What is the two-letter country code for this unit?
[Unknown]: RU
```

```
Is <CN=ibank.bankname.ru, OU=IT Department, O=Bankname, L=Moscow, ST=Russia,
C=RU> correct?
[no]: yes
```

```
Enter key password for <ibank> (RETURN if same as keystore password):
<Введите пароль, указанный в первом запросе>
```

Внимание!

Пароль на хранилище ключей (keystore password) и пароль на секретный ключ (key password) должны совпадать.

В результате работы утилиты в каталоге `$SERVER_ROOT/conf` будет создан файл хранилища — `.sslkeystore`

Генерация и отправка запроса на получение SSL-сертификата

Для генерации запроса на получение SSL-сертификата запустите утилиту `keytool` с параметрами:

```
$JAVA_HOME/bin/keytool -certreq -alias ibank -file $SERVER_ROOT/conf/certreq.csr
-keystore $SERVER_ROOT/conf/.sslkeystore
```

где

`{-alias ibank}` — псевдоним (имя), под которым ваш сертификат находится в хранилище. В данном примере — `ibank`;

`{-file $SERVER_ROOT/conf/certreq.csr}` — файл, в который следует поместить информацию о запросе после его создания. В данном примере — `$SERVER_ROOT/conf/certreq.csr`;

`{-keystore $SERVER_ROOT/conf/.sslkeystore}` — путь к файлу с SSL-хранилищем. В данном примере — `$SERVER_ROOT/conf/.sslkeystore`;

В процессе работы утилита запросит пароль. Необходимо использовать пароль, заданный при генерации хранилища.

В результате работы утилиты в каталоге `$SERVER_ROOT` будет сформирован файл `certreq.csr`, который необходимо отправить в Сертификационный Центр.

Полученный на основе запроса SSL-сертификат необходимо импортировать в хранилище.

Импорт SSL-сертификата в хранилище

Для того чтобы операция импорта сертификата прошла успешно, сначала выполняется импорт корневого сертификата, а затем, при необходимости, промежуточного.

Импорт корневого сертификата, например, `UTNAddTrustServerCA.crt`:

```
$JAVA_HOME/bin/keytool -import -trustcacerts -alias root -file
UTNAddTrustServerCA.crt -keystore $SERVER_ROOT/conf/.sslkeystore Trust this
certificate? [no]: yes
```

Импорт промежуточного сертификата, например, `RBCHCHighAssuranceServices.crt`:

```
$JAVA_HOME/bin/keytool -import -trustcacerts -alias INTER -file
RBCHCHighAssuranceServices.crt -keystore $SERVER_ROOT/conf/.sslkeystore Enter
keystore password: <Пароль на хранилище ключей>
```

Импорт доменного сертификата, например, `RBCHCGoldSSLCertificate.crt`, полученного от Хостинг Центра РБК:

```
$JAVA_HOME/bin/keytool -import -trustcacerts -alias ibank -file
RBCHCGoldSSLCertificate.crt -keystore $SERVER_ROOT/conf/.sslkeystore Enter
keystore password: <Пароль на хранилище ключей>
```

Создание самозаверенного SSL-сертификата

Самозаверенный SSL-сертификат — это сертификат, выданный банком самому себе. Его использование допустимо только в период опытной эксплуатации системы "iBank для Бизнеса".

После [создания хранилища секретных ключей](#) необходимо провести самостоятельное заверение SSL-сертификата, выполнив команду:

```
$JAVA_HOME/bin/keytool -selfcert -alias ibank -keystore $SERVER_ROOT/
conf/.sslkeystore -validity 730
```

Далее экспортируйте сертификат из хранилища секретных ключей в файл формата `der`, выполнив команду:

```
$JAVA_HOME/bin/keytool -export -alias ibank -keystore $SERVER_ROOT/
conf/.sslkeystore -file $SERVER_ROOT/CaCert2048.der
```

В результате будет создан файл `$SERVER_ROOT/CaCert2048.der` с самозаверенным сертификатом банка.

Этот файл необходимо будет передать доверенным путем пользователям системы перед их началом работы во время опытной эксплуатации для установки в web-браузеры.

Шаг 8. Конфигурирование сервера приложений "iBank для Бизнеса"

Конфигурирование серверов приложений выполняется в модуле "Конфигуратор системы для юридических лиц".

Основное назначение модуля "Конфигуратор системы для юридических лиц":

- управление кластером серверов приложений системы "iBank для Бизнеса";
- добавление серверов приложений в кластер;
- управление распределением серверных модулей по серверам приложений;
- конфигурирование подключения к БД;
- конфигурирование точек обращения корпоративных клиентов к банковской системе "iBank для Бизнеса";
- управление настройками журналирования;
- настройка системных свойств;
- загрузка файла Лицензии;
- настройка реквизитов банков и филиалов;
- регистрация сертификата ключа проверки ЭП главного администратора системы. Ему делегируются права по управлению клиентами и сотрудниками головного банка, а также регистрация администраторов филиалов;
- управление OTP- и MAC-токенами;
- обновление прошивки Интернет-Банка, обновление xslt-шаблонов SMS-Банка, обновление шаблонов выгрузки документов в Excel;
- настройка взаимодействия с внешними сервисами.

Запуск модуля "Конфигуратор системы для юридических лиц"

Индивидуальная настройка Java для модуля "Конфигуратор системы для юридических лиц"

Если вы **не** используете для Java переменных системного окружения, то раскомментируйте и установите значение переменной `JAVA_HOME` в командном файле `$SYSCON_ROOT/bin/setvars.sh`, где `$SYSCON_ROOT` это каталог с установленным модулем.

Запуск модуля "Конфигуратор системы для юридических лиц" выполняется запуском командного файла `$SYSCON_ROOT/bin/syscon.sh`. При этом на экран выводится диалоговое окно **Конфигуратор системы**, внешний вид которого представлен на [рис. 3](#).

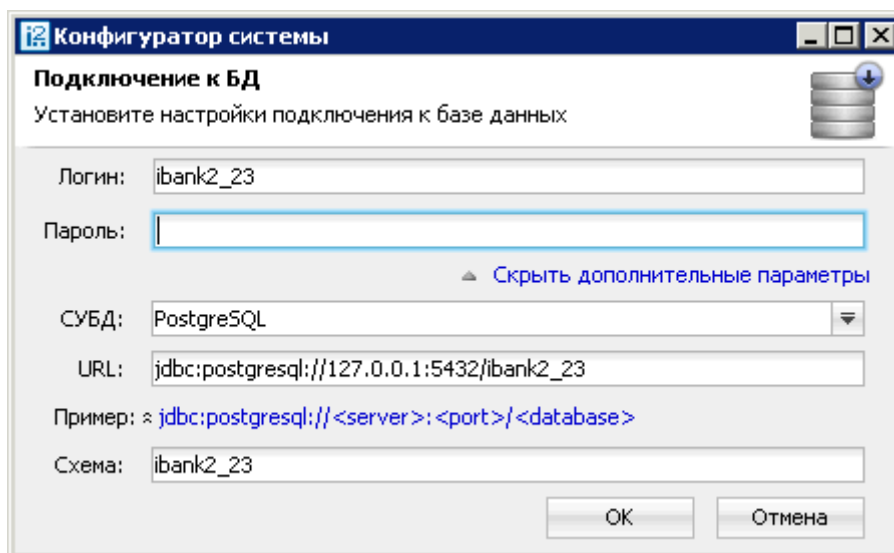


Рис. 3. Вход в модуль "Конфигуратор системы для юридических лиц"

В окне **Конфигуратор системы** укажите логин и пароль владельца объектов БД "iBank для Бизнеса" и нажмите кнопку **ОК**.

По ссылке **Показать дополнительные параметры** отображаются поля с параметрами подключения к БД "iBank для Бизнеса", которые берутся из конфигурационного файла \$SYSCON_ROOT/conf/connection.xml

После успешного подключения на экран выведется основное окно **Конфигуратор системы**, внешний вид которого представлен на [рис. 4](#).

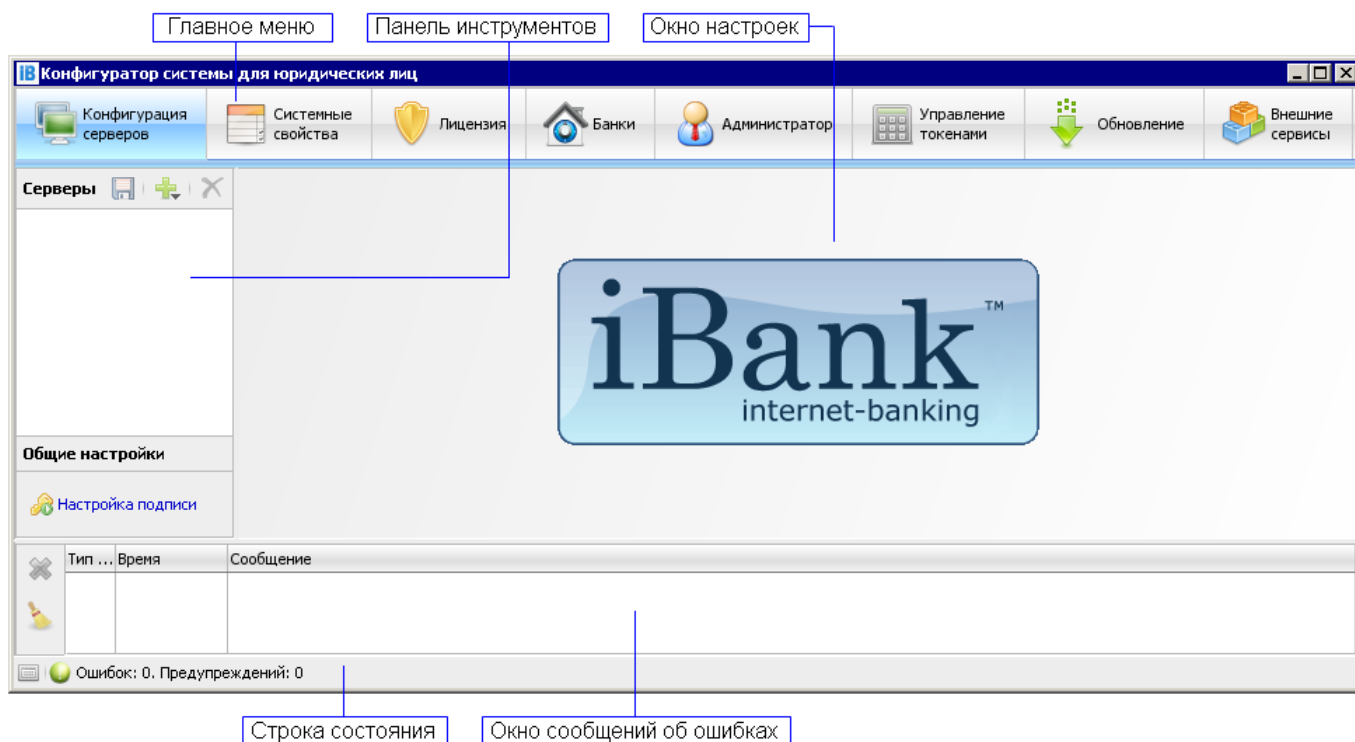


Рис. 4. Основное окно модуля "Конфигуратор системы для юридических лиц"

Установка Лицензии

В системе "iBank для Бизнеса" лицензируются:

- количество серверов приложений;
- количество клиентов;
- серверные модули;
- файловые СКЗИ.

Подробнее см. в разделе «Лицензирование».

Установка и обновление состава Лицензии выполняется в разделе **Лицензия** модуля "Конфигуратор системы для юридических лиц" (см. [рис. 5](#)).

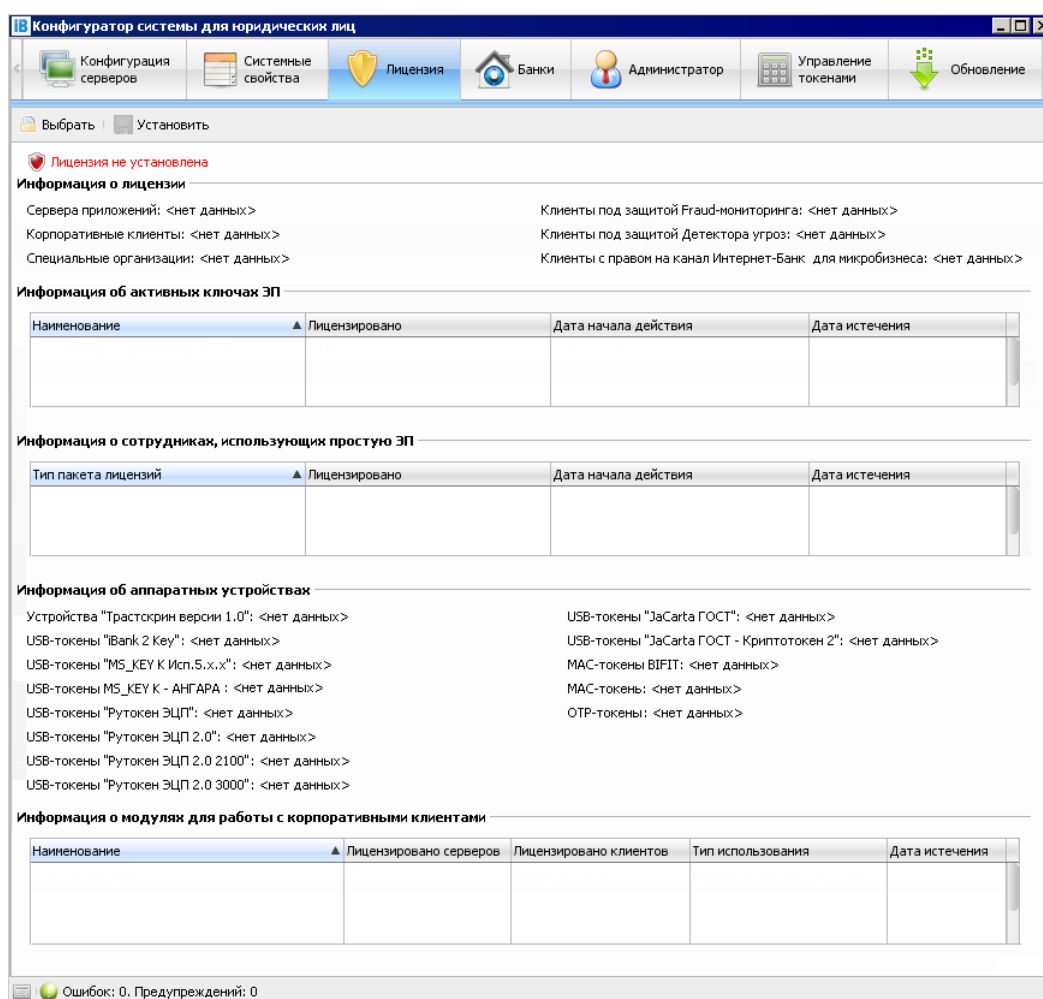




Рис. 5. Раздел "Лицензия" модуля "Конфигуратор системы для юридических лиц"

Для установки Лицензии нажмите кнопку  **Выбрать** панели инструментов: откроется стандартное диалоговое окно выбора файлов, в котором выберите полученный от компании "БИФИТ" файл Лицензии — `license.dat` Затем нажмите кнопку  **Установить** панели инструментов. Лицензия будет установлена и информация о ее составе отразится в окне настроек модуля (см. [рис. 6](#)).

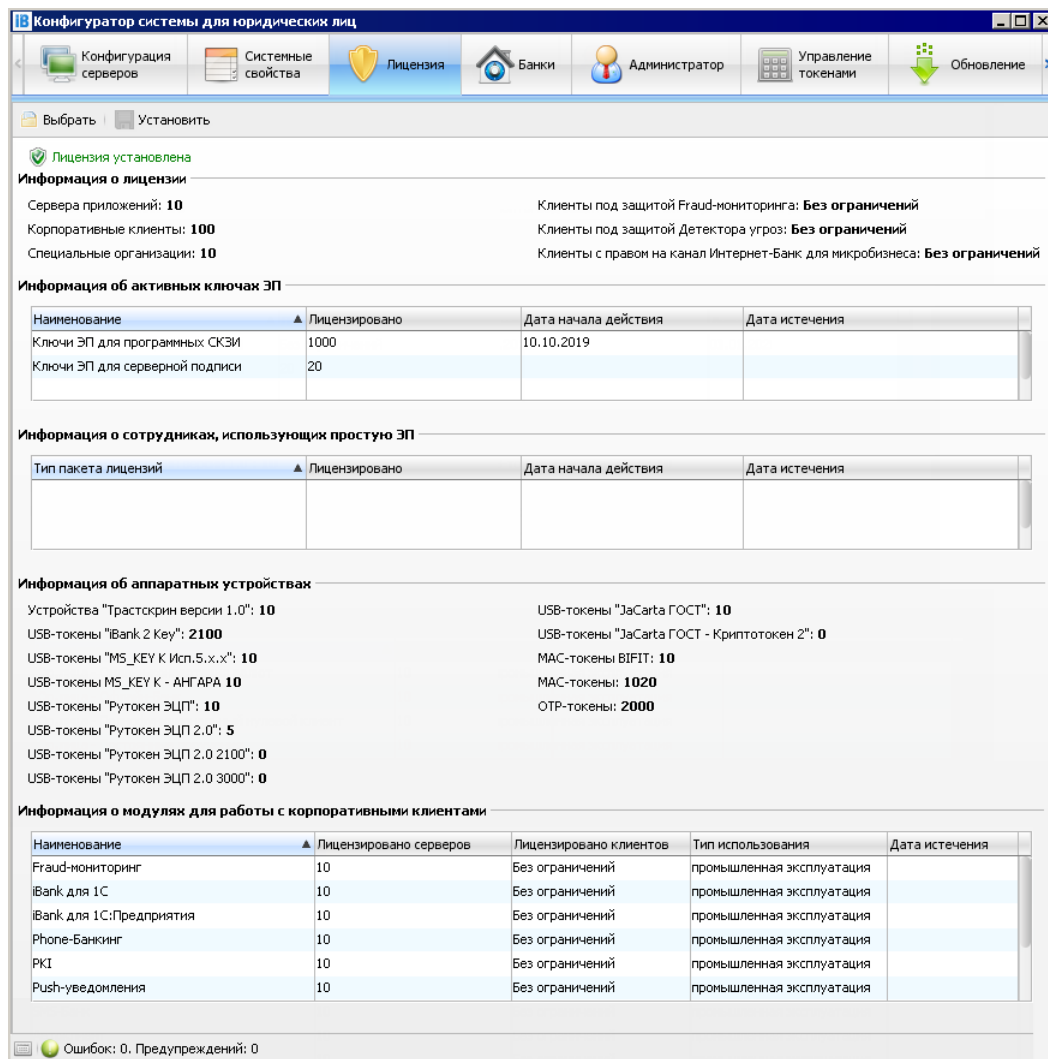


Рис. 6. Раздел "Лицензия" модуля "Конфигуратор системы для юридических лиц"

Лицензирование

- Лицензирование ключей ЭП программных СКЗИ [23];
- Лицензирование простых ЭП [25];
- Лицензирование количества клиентов в лицензиях на серверные модули [25];
- Механизм контроля количества свободных лицензий [26];

Лицензирование ключей ЭП программных СКЗИ

Лицензируется общее количество активных ключей ЭП клиентов и сотрудников банка:

- "Файловых";
- "Облачных";
- КЭП и "сторонних".

Ключи ЭП в USB-токенах и MAC-токенах BIFIT не лицензируются.

Лицензированию подлежит каждый ключ ЭП, созданный при помощи программных СКЗИ:

- Крипто-Ком 3.3;
- Крипто-Ком 3.4 исп. 40, 41;
- Крипто-Ком 3.4 исп. 42, 43;

- Крипто-Ком 3.5;
- КриптоПро CSP;
- Signal-ComCSP;
- VipNetCSP.

Обращаем внимание, что использование СКЗИ, а также созданные с их помощью ключи ЭП, с истекшим сроком действия сертификатов соответствия, выданных ФСБ РФ, нелегитимно.

Сведения о срочных и бессрочных лицензиях на ключи ЭП программных СКЗИ отображаются:

- в модуле "Конфигуратор системы для юридических лиц":
 - в пункте "Информация об активных ключах ЭП" (см. рис. 6).
- в модуле "Администратор банка/филиала":
 - в разделе Информация/ Лицензии отображается общее количество лицензированных ключей ЭП для программных СКЗИ (см. рис. 7);
 - в разделе Информация/ Лицензируемые ключи ЭП отображается общее количество лицензируемых ключей ЭП соответствующего типа в разрезе организации (см. рис. 8).

	Лицензировано	Зарегистрировано	Доступно
Корпоративные клиенты	100	18	82
Клиенты под защитой Fraud-мониторинга	-	4	-
Клиенты под защитой Детектора угроз	-	0	-
Информационные клиенты	-	7	-
Специальные организации	10	0	10
Сотрудники, использующие простую подпись	0	0	0
Активные ключи ЭП для серверной подписи	20	0	20
Активные ключи ЭП для программных СКЗИ	1000	21	979
Устройства "Трастскрин версии 1.0"	10	1	9
USB-токены "iBank 2 Key"	2100	1	2099
USB-токены "MS_KEY К Исп.5.хх"	10	0	10
USB-токены MS_KEY К - АНГАРА	10	4	6
USB-токены "Рутокен ЭЦП"	10	0	10
USB-токены "Рутокен ЭЦП 2.0"	5	0	5
USB-токены "Рутокен ЭЦП 2.0 2100"	0	0	0
USB-токены "Рутокен ЭЦП 2.0 3000"	0	0	0
USB-токены "JaCarta ГОСТ"	10	0	10
USB-токены "JaCarta ГОСТ - Криптотокен 2"	0	0	0
MAC-токены BIFIT	10	1	9
MAC-токены	1020	3	1017
OTP-токены	2000	1	1999

Рис. 7. Модуль "Администратор банка/филиала", диалог "Информация о лицензиях"

ИНН	Наименование клиента	Облачные	Файловые	Сторонние
9710059358	АО "Крокус"	1	2	
7719610018	АО Дизайн			
7419636548...	ЗАО "Березка"			
7418529637	ЗАО "Кипарис"			
1234567890...	ИП Иванов Иван Иванович			
7713661800	ИП Кирьянов Виктор Петрович		2	
2134214124	ООО "Гранит"			
7723123456	ООО "Демоклиент"	8	3	
7712021214	ООО "Стрела"			
7701010101	ООО "Фигус"			
1234123412	ООО Ромашка			
7704595727	ООО Чашка			

Всего ключей ЭП (с учетом банковских и ЦФК): 21
Лицензировано ключей ЭП: 1000

Рис. 8. Модуль "Администратор банка/филиала", диалог "Информация о лицензируемых ключах ЭП"

В модуле "Администратор банка/филиала" после регистрации подлежащего лицензированию ключа ЭП или исполнения "Заявления на выпуск сертификата"/ "Заявления об использовании Электронной подписи" отображаются предупреждения:

- если выявлен недостаток количества лицензий на ключи:

"Внимание! Исчерпана лицензия на ключи ЭП для <тип ключа ЭП>. Сервер будет остановлен ДД.ММ.ГГГГ";

- если выявлено, что осталось менее 5% или менее 10 свободных лицензий:

"Внимание! Доступно X лицензий на ключи ЭП. Чтобы избежать остановки сервера, своевременно приобретите дополнительные лицензии".

Лицензирование простых ЭП

Распространяется на количество сотрудников, использующих простую электронную подпись. Возможны два типа пакетов лицензий:

- С ограничением количества клиентов;
- Без ограничения количества клиентов.

Сведения о лицензиях простых ЭП доступны:

- в модуле "Конфигуратор системы для юридических лиц":

— в пункте "Информация о сотрудниках, использующих простую ЭП" (см. [рис. 6](#));

— в пункте "Информация о модулях для работы с корпоративными клиентами" для разграничения наименований лицензий на серверный модуль "Сервер подписи ВІFІТ" может отображаться значение (см. [рис. 6](#)):

Сервер подписи ВІFІТ (простая ЭП);

Сервер подписи ВІFІТ (облачная ЭП).

- в модуле "Администратор банка/филиала":

— в разделе Информация/ Лицензируемые ключи ЭП отображается общее количество лицензируемых ключей ЭП соответствующего типа в разрезе организации (см. [рис. 8](#)).

Лицензирование количества клиентов в лицензиях на серверные модули

Возможны два типа пакетов лицензий:

- С ограничением количества клиентов;
- Без ограничения количества клиентов.

Сведения о количестве клиентов в лицензиях на серверные модули отображаются:

- в модуле "Конфигуратор системы для юридических лиц":

— в пункте "Информация о модулях для работы с корпоративными клиентами" в столбце "Лицензировано клиентов" (см. [рис. 6](#)). Возможные значения:

Число. Соответствует количеству клиентов, на которое лицензирован серверный модуль или канал обслуживания.

Без ограничений. В лицензии на модуль нет ограничений на количество клиентов.

- в модуле "Администратор банка/филиала":

— в разделе Информация/ Лицензии сведения о лицензиях отображаются в виде Лицензировано-Зарегистрировано-Доступно (см. [рис. 7](#)).

Механизм контроля количества свободных лицензий

Возможные действия при выявлении превышения лицензированного количества клиентов в лицензиях:

- Остановка серверного модуля при превышении числа клиентов с правом на канал обслуживания/ на серверный модуль над количеством лицензированных клиентов;

Применяется для каналов обслуживания:

- Интернет-Банк;
- Интернет-Банк для микробизнеса;
- Тикер;
- SMS-Банк;
- Корпоративный автоклиент;
- Мобильный банк;
- Мобильный банк (информационная версия)

Применяется для серверных модулей:

- Банковский ассистент;
- Push-уведомления;
- Нулевой клиент;
- Полнофункциональный нулевой клиент;
- Витрина услуг;
- Конверсионные операции во внешней системе;
- Конструктор документов;
- Конструктор документов клиента;
- Конструктор документов банка;
- Конструктор двухсторонних документов;
- Чат для бизнеса WEB (Webim);
- Чат для бизнеса Mobile (Webim);
- Конструктор документов Мобильного банка;
- Корпоративные карты;
- Зарплатный проект для микробизнеса;
- Чат для микробизнеса WEB (Webim);
- Чат для микробизнеса Mobile (Webim);
- Корпоративные карты для микробизнеса;
- Операции по кредитам для микробизнеса;
- Конструктор документов клиента для микробизнеса;
- Конструктор документов банка для микробизнеса;
- Конструктор документов Мобильного банка для микробизнеса;
- Онлайн-конвертация валют в Мобильном банке;
- Зарплатные проекты;

- Кредиты;
 - Депозиты;
 - Онлайн-конвертация валют;
 - Онлайн-конвертация валют по непрерывно транслируемым курсам;
 - Постоянные поручения.
- Остановка сервера приложений при превышении числа клиентов над количеством лицензированных клиентов.
- Применяется для продуктов:
- Fraud-мониторинг;
 - Детектор угроз.

Примечание:

Для не упомянутых лицензий, используется аналогичный механизм контроля за превышением количества лицензированных клиентов.

При превышении количества любых лицензий дается до **14** дней, чтобы обновить количество лицензий. Работа сервера приложений разрешена до истечения этого срока.

Электронные адреса, на которые осуществляется отправка сообщений об исчерпании количества лицензий и о сроках отключения сервера приложений, указываются в свойстве `certificate.excess_licensed_info.email`

На адрес support@bifit.com отправляется идентичное сообщение.

Создание конфигурации сервера приложений

Конфигурирование серверов приложений выполняется в разделе **Конфигурация серверов** модуля "Конфигуратор системы для юридических лиц" (см. [рис. 9](#)).



Вносимые изменения в процессе конфигурирования сервера приложений должны быть сохранены в БД системы "iBank для Бизнеса". Во время запуска сервера приложений его конфигурационные файлы обновляются в соответствии с параметрами конфигурации, сохраненной в БД. Сохранение выполняется нажатием кнопки  панели инструментов секции **Серверы**.



Рис. 9. Раздел "Конфигурация серверов" модуля "Конфигуратор системы для юридических лиц"

Добавление сервера приложений

Для добавления сервера в секции **Серверы** (левая часть раздела **Конфигурация серверов**) нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Добавить/сервер приложений**. В открывшемся окне **Добавление хоста** (см. рис. 10) укажите уникальное наименование хоста и нажмите кнопку **ОК**.

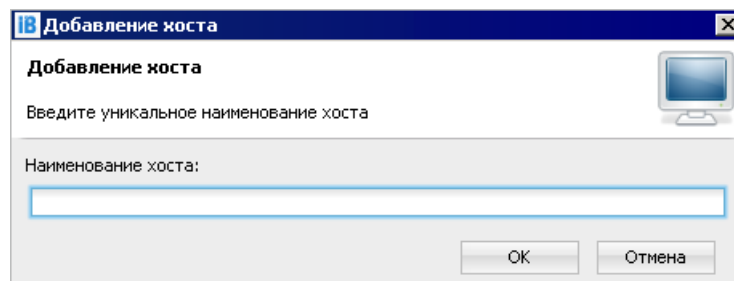


Рис. 10. Окно "Добавление хоста"

Желательно, чтобы наименование хоста совпадало с именем компьютера, на котором разворачивается сервер приложений.

В случае указания несовпадающих имен необходимо раскомментировать и установить значение переменной `name` в конфигурационном файле `$SERVER_ROOT/conf/hostname.properties`

После сохранения наименования хоста в секции **Конфигурация** (правая часть раздела **Конфигурация серверов**) отобразится структура конфигурации сервера приложений (см. рис. 11).

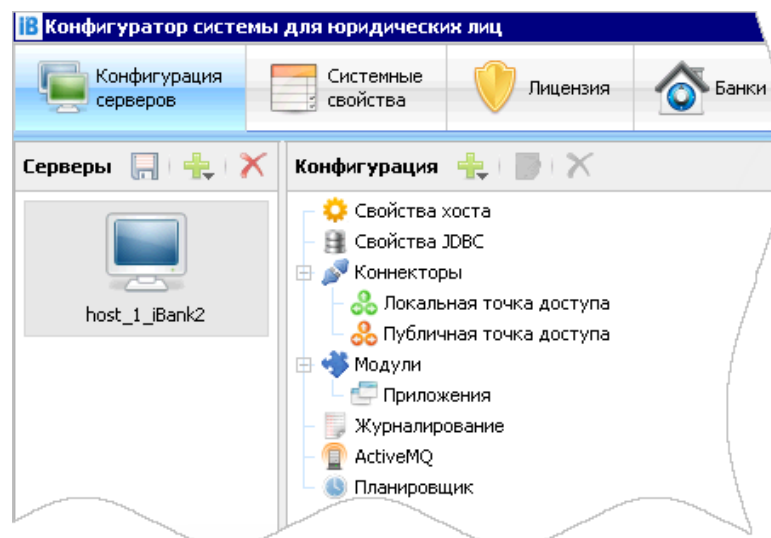


Рис. 11. Структура конфигурации сервера приложений

Далее необходимо выполнить настройку сервера приложений и сохранить его конфигурацию в БД системы "iBank для Бизнеса".

При запуске сервера приложений параметры его конфигурации будут взяты из БД.

Примечание:

Используйте несколько серверов приложений для разграничения сетевого пространства работы клиентов банка и банковских сотрудников. Конфигурируйте один сервер для обработки запросов от модулей клиентов банка из внешней сети (Интернет), а другой — для обработки запросов от модулей банковских сотрудников из внутрибанковской сети.

Добавление сервера на основе существующего

В секции **Серверы** выберите сервер, вызовите контекстное меню и выберите пункт **Создать копию** (см. рис. 12). В открывшемся окне укажите уникальное наименование хоста и нажмите кнопку **ОК**.

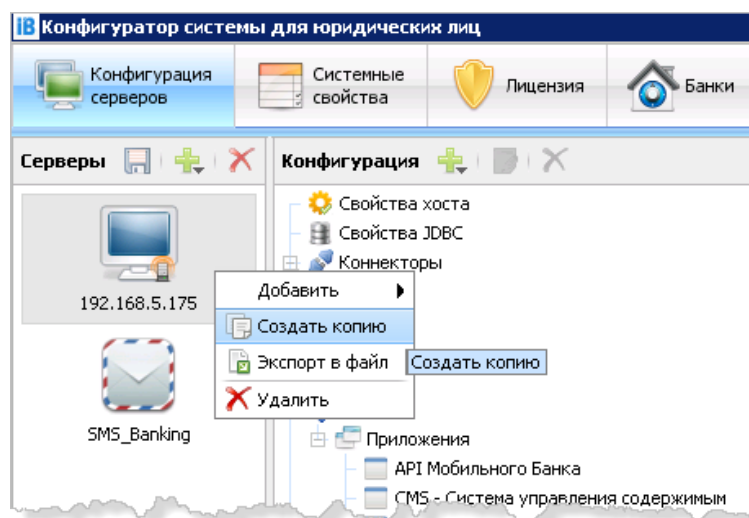


Рис. 12. Создание копии конфигурации сервера приложений

Экспорт конфигурации сервера приложений в файл

В секции **Серверы** выберите сервер, вызовите контекстное меню и выберите пункт **Экспорт в файл** (см. рис. 13). В открывшемся окне укажите имя файла и каталог сохранения файла конфигурации, нажмите кнопку **ОК**. По умолчанию имя файла будет идентично имени хоста, расширение файла "hc", например 192.168.5.175.hc.

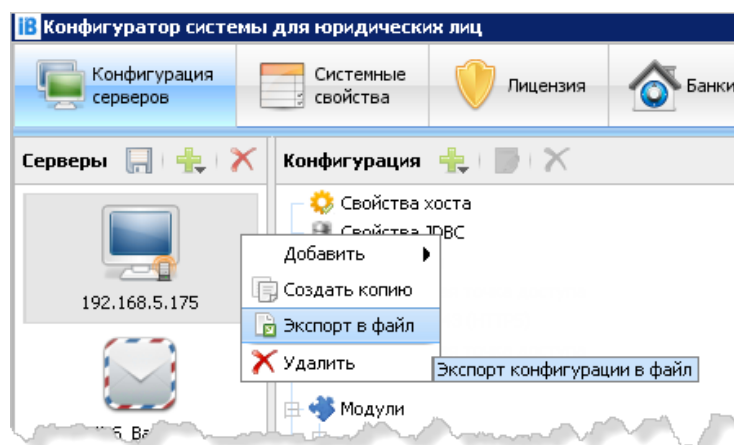



Рис. 13. Экспорт конфигурации сервера приложений в файл

Настройка свойств хоста сервера приложений

Настройка свойств хоста сервера приложений выполняется в пункте **Свойства хоста** структуры конфигурации выбранного сервера приложений. Значения свойств хоста устанавливаются автоматически в момент добавления сервера приложений.

Для изменения свойств хоста выберите пункт **Свойства хоста** секции **Конфигурация** и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Редактировать**.

В открывшемся окне **Свойства хоста** на закладке **Свойства** отображаются значения: наименование хоста, порт остановки и параметры JVM, на закладке **AGI-сервер** задаются параметры AGI-сервера: использовать AGI, адрес сервера, порт, минимальное и максимальное число потоков (см. рис. 14).

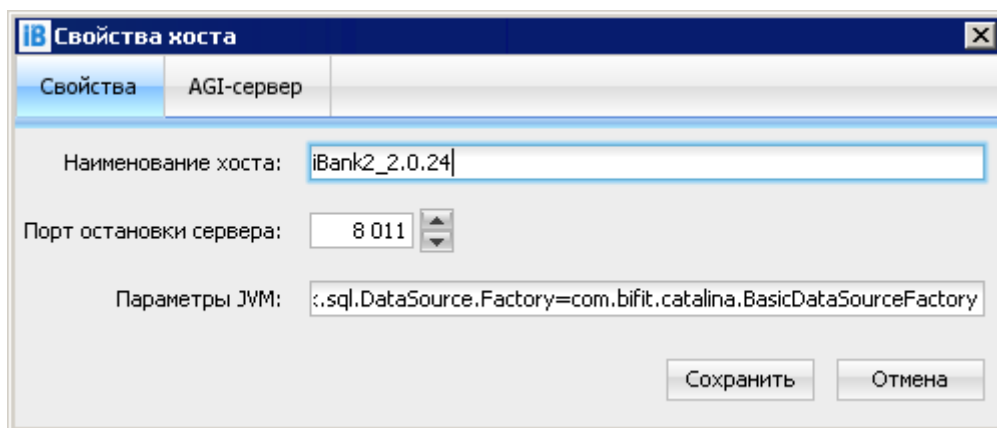


Рис. 14. Окно "Свойства хоста"

После ввода наименования хоста и нажатия кнопки **Сохранить** появится сообщение с предложением загрузить типичные настройки точек доступа на сервер приложений (см. [рис. 15](#)).

При нажатии на кнопку **Да** устанавливается конфигурация с настроенными коннекторами публичной и локальной точек входа. При нажатии на кнопку **Нет** настройку коннекторов точек входа необходимо выполнить вручную (см. [Настройка точек доступа на сервер приложений](#)).

При создании нового экземпляра сервера приложений также возможно установить настройки по умолчанию.

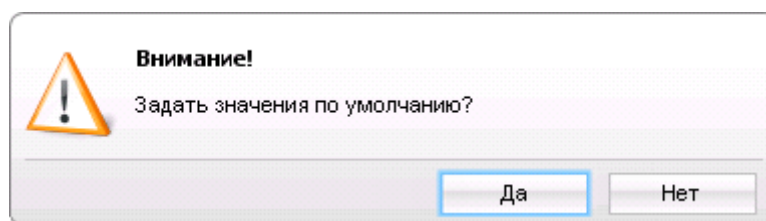




Рис. 15. Окно загрузки настроек по умолчанию

При внесении изменений меняются параметры конфигурации сервера приложений. Для сохранения измененной конфигурации нажмите кнопку  панели инструментов секции **Серверы**. Для сервера изменения вступят в силу после его перезапуска.

Настройка свойств пула соединений сервера приложений

Настройка свойств пула соединений сервера приложений с БД системы "iBank для Бизнеса" выполняется в пункте **Свойства JDBC** структуры конфигурации выбранного сервера приложений. Первоначально значения свойств устанавливаются автоматически при добавления сервера приложений.

Для изменения свойств пула соединений выберите пункт **Свойства JDBC** секции **Конфигурация** и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Редактировать**.

В открывшемся окне **Свойства JDBC** отображаются значения параметров, заданные по умолчанию (см. [рис. 14](#)).

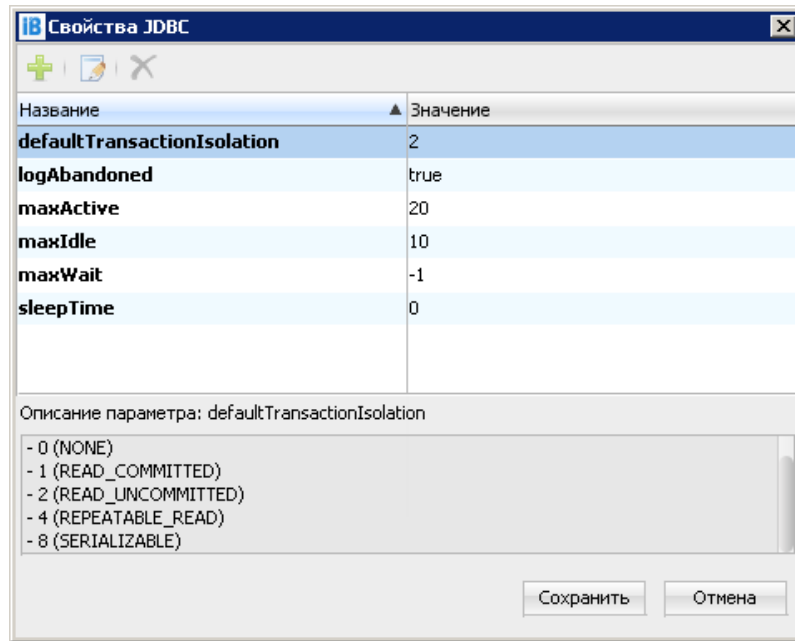



Рис. 16. Окно "Свойства JDBC"

Для добавления параметра:

1. Нажмите кнопку 
2. В отобразившемся окне **Добавление параметра jdbc-пула** выберите параметр из выпадающего списка **Название** (см. рис. 17).

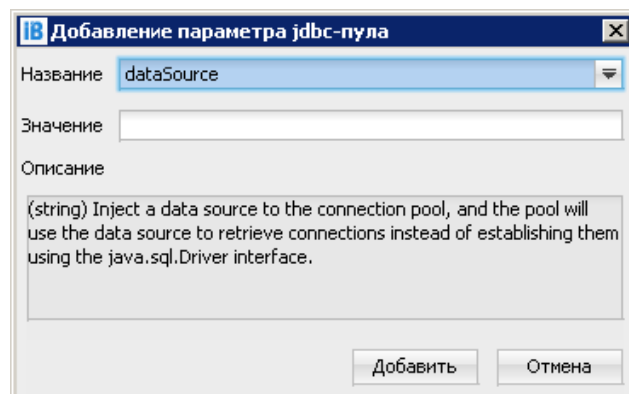



Рис. 17. Окно "Добавление параметра jdbc-пула"

3. Укажите значение параметра в соответствующем поле.
4. Нажмите кнопку **Добавить**.

Если сервер приложений запускается раньше, чем СУБД, установите значение таймаута, отличное от 0 для параметра **sleepTime**. Значение устанавливается в миллисекундах.

При внесении изменений меняются параметры конфигурации сервера приложений. Для сохранения измененной конфигурации нажмите кнопку  в секции **Серверы**. Для сервера изменения вступят в силу после его перезапуска.


Настройка точек доступа на сервер приложений

Для работы сервера приложений необходимо наличие двух точек доступа:

- **Публичная точка входа.** Через эту точку с сервером приложений взаимодействуют корпоративные клиенты банка, работающие через интернет с использованием HTTPS-

протокола (мобильные и web-приложения, "Корпоративный автоклиент" и "Тикер для корпоративных клиентов").

- **Локальная точка входа.** Через эту точку с сервером приложений взаимодействуют банковские сотрудники, работающие из внутреннего защищенного банковского сегмента, с использованием HTTPS-протокола (web-приложения, java-приложение "Администратор банка/филиала").

Для настройки точки доступа выберите ее и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Редактировать**.

Откроется окно **Свойства точки доступа** (см. [рис. 18](#)), в котором выполните:

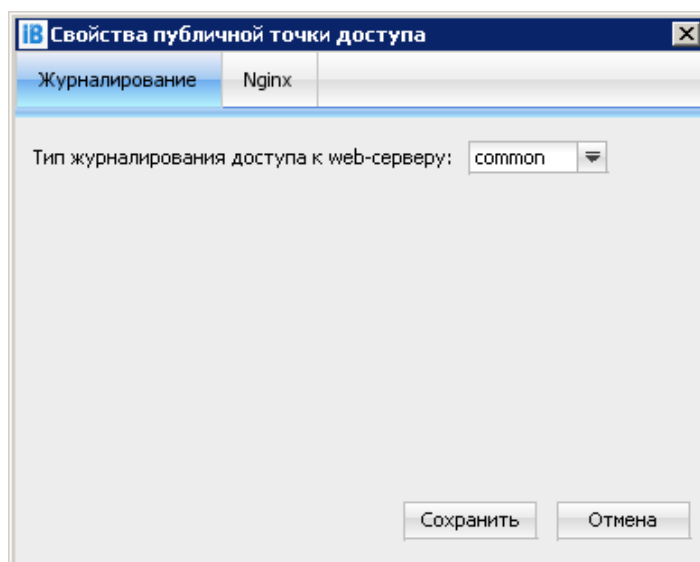


Рис. 18. Окно "Свойства публичной точки доступа". Закладка "Журналирование"

На закладке **Журналирование** укажите параметры:

- **Тип журналирования доступа к web-серверу** — выбор полей HTTP-запроса и ответа, которые выводятся в файл `access.log`: **common** или **combined**.

При выборе типа **common** выводятся заголовки HTTP-запроса:

- IP-адрес клиента;
- имя удаленного пользователя (всегда " - ");
- идентификатор ключа пользователя при успешной аутентификации, иначе " - ";
- дата и время запроса;
- применяемый метод протокола HTTP;
- запрашиваемый ресурс;
- код ответа протокола HTTP;
- количество переданных байт.

При выборе типа **combined** дополнительно к полям типа **common** выводятся заголовки HTTP-запроса:

- URL источника запроса;
- наименование клиентского приложения, приславшего запрос.

На закладке **Nginx** (только для публичной точки доступа) при необходимости выполните настройку прокси-сервера, в качестве которого выступает сервер nginx (см. [рис. 19](#)).

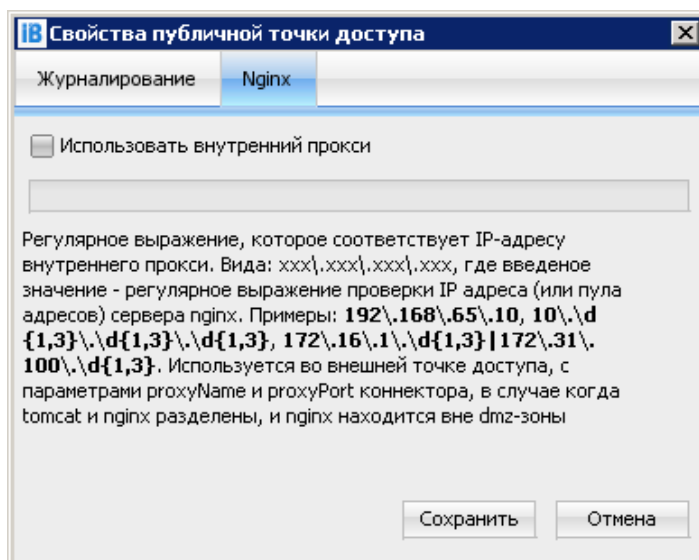


Рис. 19. Окно "Свойства публичной точки доступа". Закладка "Nginx"

Настройка выполняется в следующих случаях:

- если сервер nginx располагается не в DMZ;
- если IP-адрес сервера nginx не соответствует следующему виду:
 - 10.*.*.*
 - 192.168.*.*
 - 169.254.*.*
 - 127.*.*.*


Для настройки выполните:

- Установите флаг **Использовать внутренний прокси**.
- Укажите регулярное выражение, вида: 1\.\2\.\3\.\4, которое соответствует IP-адресу сервера nginx.

Сохраните внесенные изменения.

Настройка коннекторов точки доступа

Под коннектором понимается тип протокола, по которому происходит взаимодействие между сервером приложений и клиентскими модулями системы.

Для добавления коннектора нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Добавить/ Коннектор**.

В открывшемся окне **Новый коннектор** (см. [рис. 20](#)) выберите параметры добавляемого коннектора:

- **Тип** — тип точки доступа: локальный или публичный.
- **Протокол** — протокол взаимодействия между сервером приложений и клиентскими модулями системы:

Протоколы **HTTP**,
HTTPS

используются для обращения к серверу приложений клиентами и банковскими сотрудниками при работе с мобильными и web-приложениями системы.

Протокол **SSLRouter** используется для обработки HTTPS-запросов при подключении к серверу приложений через Центр очистки трафика "ИБАНК2. РУ"¹

¹Подробную информацию о Центре очистки трафика "ИБАНК2. РУ" вы можете получить у специалистов компании "БИФИТ"

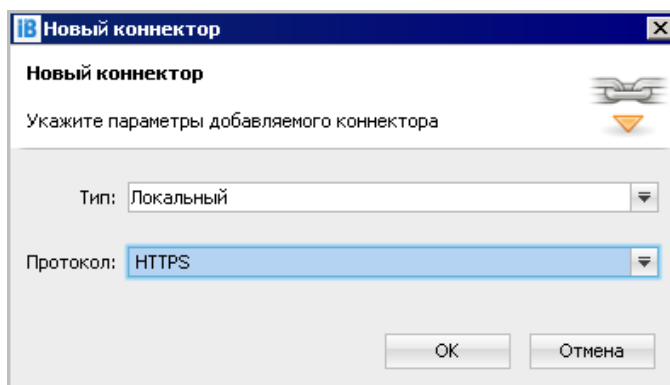


Рис. 20. Окно "Новый коннектор"

После добавления коннектора откроется окно настроек (см. рис. 21), в котором должны быть указаны параметры:

- **address** — адрес доступа к серверу приложений. Указывается только для локальной точки доступа. Адрес должен быть доступный только из внутренней сети банка.




В качестве адресов коннекторов также могут указываться доменные имена, если соответствующим образом сконфигурирован DNS-сервер.

Адрес коннектора точки доступа может быть не задан явно. В этом случае подключение к серверу приложений будет возможно по всем адресам сетевых интерфейсов, существующих на данном компьютере.

- **certificateKeystoreAlias** — имя используемого ключа из хранилища ключей публичной и локальной точки доступа.
- **certificateKeystoreFile** — путь к хранилищу ключей `.sslkeystore`. Указывается для HTTPS-протокола публичной и локальной точки доступа.
- **certificateKeystorePassword** — пароль для доступа к хранилищу ключей `.sslkeystore`. Указывается для HTTPS-протокола публичной и локальной точки доступа.
- **port** — порт доступа к серверу приложений. Для *локальной* точки по умолчанию устанавливается порт **9443** для HTTPS-протокола. Для *публичной* точки по умолчанию устанавливается порт **443** для HTTPS-протокола.

Сохраните внесенные изменения.

Параметры, значения которых заданы по умолчанию, можно редактировать, а также добавлять новые свойства из списка доступных.

Для добавления свойства коннектора нажмите кнопку  в окне (см. рис. 21). Для редактирования свойства коннектора выберите его из списка и нажмите кнопку , для удаления свойства нажмите кнопку .

Для просмотра скрытых параметров установите флаг в поле **Показывать скрытые параметры**.

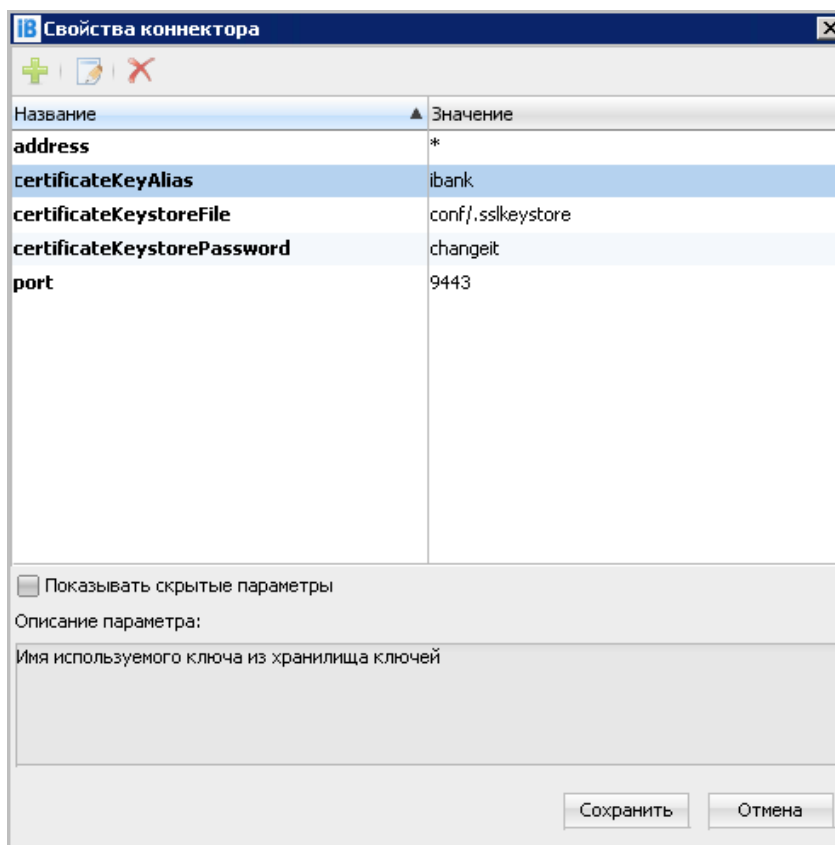



Рис. 21. Окно "Свойства коннектора" локальной точки доступа

Настройка клиентских приложений системы

Настройка клиентских приложений системы "iBank для Бизнеса" выполняется в пункте **Модули** структуры конфигурации выбранного сервера приложений и через свойства.

Добавление приложений на сервер приложений

Вы можете разделять запросы от клиентских модулей Интернет-Банка, приложений для банковских сотрудников в необходимой пропорции между серверами приложений. Таким образом, можно разграничить сетевое пространство работы клиентов банка и банковских сотрудников, т.к. первые работают из внешней сети (Интернет), а вторые только из внутрибанковской сети. Это позволяет увеличить общую производительность, повысить надежность и обеспечить непрерывность работы системы.

Для добавления приложений на сервер приложений в секции **Конфигурация** нажмите кнопку  панели инструментов и выберите подпункт **Приложение** или вызовите контекстное меню и выберите пункт **Добавить/ приложение**.

В открывшемся окне **Добавление приложений** отметьте необходимые приложения системы: черным цветом отображаются приложения, доступные в рамках Лицензии (см. [рис. 22](#)). Для выбора всех доступных приложений проставьте флаг в поле **Наименование**

Нажмите кнопку **ОК** для сохранения внесенных изменений.

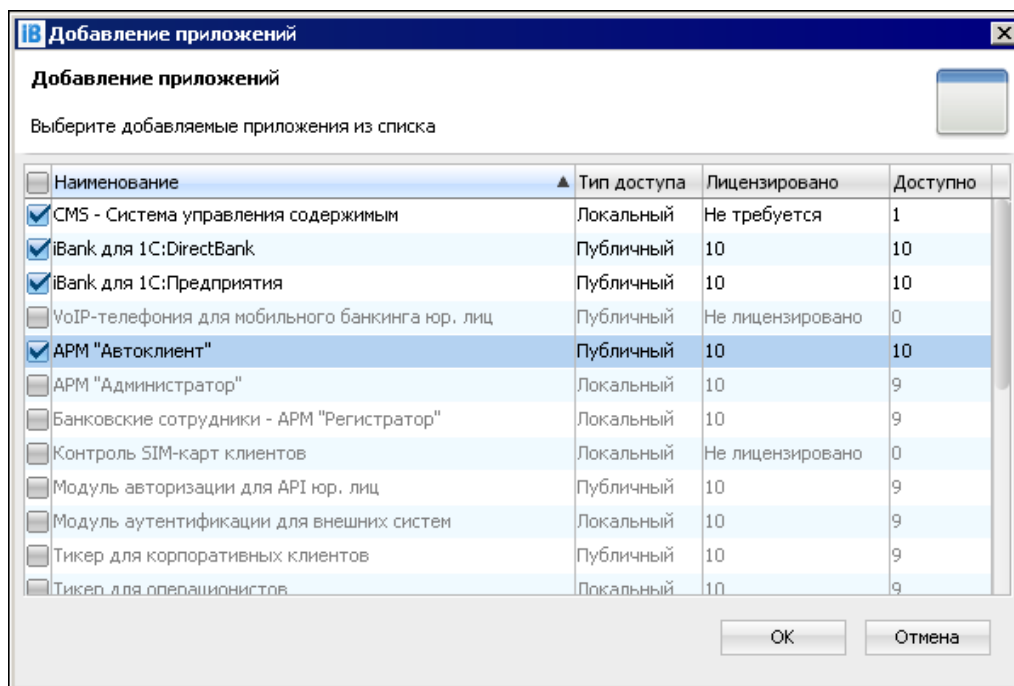



Рис. 22. Окно "Добавление приложений"

Для удаления приложения из списка выберите необходимое и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Удалить**.

Настройка точек доступа для клиентских модулей

Настройка адреса точек доступа для подключения клиентских модулей выполняется в разделе **Системные свойства** модуля "Конфигуратор системы для юридических лиц" в свойствах:

`ibank.administrator.url` — URL для подключения модуля "Администратор банка/ филиала". Значение необходимо задавать в формате `https://ibank.bankname.ru[:port]`

`ibank.client.ticker.url` — URL для подключения модуля "Тикер для корпоративных клиентов". Значение необходимо задавать в формате `https://ibank.bankname.ru`

`ibank.operator.ticker.url` — URL для подключения модуля "Тикер для операционистов". Значение необходимо задавать в формате `https://<адрес сервера приложений>[:port]/ticker-operator`

`ibank.client.autoclient.url` — URL для подключения модуля "Корпоративный автоклиент". Значение необходимо задавать в формате `https://bank.bankname.ru[:port]`

`owa.webauthn.relying_party_id` — Домен банка для подключения модуля "Интернет-Банк для мобильных устройств". Значение необходимо указывать без протокола. Значение по умолчанию `ibank2.bankname.ru`


`owa.webauthn.origin` — Набор адресов, для которых будет доступен модуль "Интернет-Банк для мобильных устройств". Значения должны иметь протокол `https://`. Допускается перечисление нескольких значений через запятую. Значение по умолчанию `https://<relying_party_id>`

Примечание:

Если значение URL точки доступа клиентского модуля не задано в свойствах, то при генерации дистрибутива модуля будет выдано соответствующее предупреждение.

Настройка журналирования работы компонентов системы

Настройка режима ведения журналов (логов) работы компонентов системы выполняется в пункте **Журналирование** структуры конфигурации выбранного сервера приложений. Первоначально режимы устанавливаются автоматически при добавления сервера приложений.

Для изменения настроек ведения логов выберите пункт **Журналирование** секции **Конфигурация** и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Редактировать**.

В открывшемся окне **Журналирование** (см. [рис. 23](#)) отображаются: название компонента, название файла ведения его журнала и режим записи сообщений.

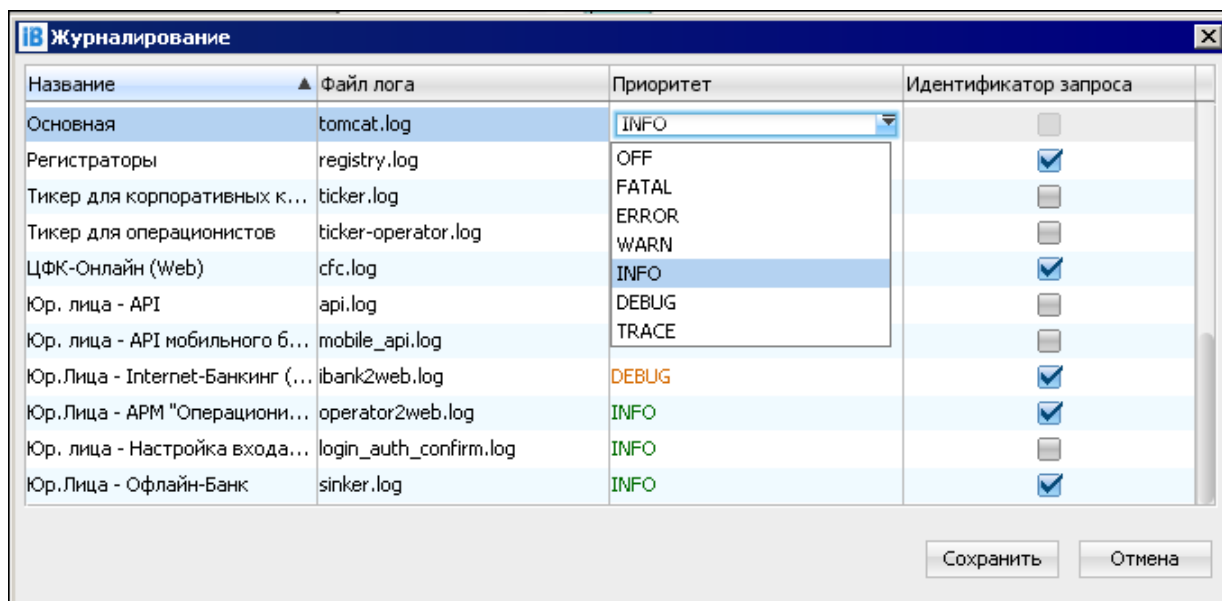



Рис. 23. Окно "Журналирование"

Для изменения типа сообщений компонента выберите необходимый из списка и в столбце **Приоритет** нажмите на кнопку  Откроется список режимов, из которого выберите необходимый:

- **OFF** — отключить все сообщения;
- **FATAL** — записывать только критические сообщения;
- **ERROR** — записывать сообщения об ошибках;
- **WARN** — записывать предупреждения;
- **INFO** — записывать информационные сообщения;
- **DEBUG** — записывать отладочную информацию;
- **TRACE** — записывать все сообщения.

В рабочем режиме рекомендуется использовать значение INFO, в процессе настройки и интеграции — более подробный режим DEBUG.

Файлы журналов сохраняются в каталог `$SYSCON_ROOT/logs` и `$SERVER_ROOT/logs`, где

- `$SYSCON_ROOT/logs` — каталог для сохранения журналов работы модуля "Конфигуратор системы для юридических лиц", журналов процедуры формирования БД системы "iBank для Бизнеса", журналов процедуры загрузки ресурсов системы "iBank для Бизнеса", журналов загрузки справочников БИК, SWIFT.
- `$SERVER_ROOT/logs` — каталог для сохранения журналов работы сервера приложений "iBank для Бизнеса" и серверных модулей системы "iBank для Бизнеса".

Список логов системы "iBank для Бизнеса" приведен в [Приложении 4](#).


Настройка брокера ActiveMQ

Настройка брокера ActiveMQ выполняется в пункте **ActiveMQ** структуры конфигурации выбранного сервера приложений.

Система "iBank для Бизнеса" использует Apache ActiveMQ в качестве очереди сообщений — компоненты, осуществляющей взаимодействие между сервером приложений и шлюзом рассылки уведомлений. ActiveMQ входит в состав сервера приложений. Подробнее об Apache ActiveMQ см. на сайте разработчика — <http://activemq.apache.org>

Шлюз рассылки уведомлений — компонент, осуществляющий доставку сообщений провайдеру, который отправляет уведомление по SMS или E-mail.

Отправка уведомлений может использоваться для оперативного получения клиентами сведений о транзакциях и остатках по их счетам и картам, а также в дополнительных механизмах безопасности системы "iBank для Бизнеса", использующих SMS и E-mail уведомления.

Для настройки свойств брокера ActiveMQ выберите пункт **ActiveMQ** секции **Конфигурация** и нажмите кнопку  панели инструментов или вызовите контекстное меню и выберите пункт **Редактировать**.

В открывшемся окне **Свойства ActiveMQ** задаются параметры SSL-коннектора и пароль на хранилище ключей JMS, необходимые для работы брокера (см. [рис. 24](#)).

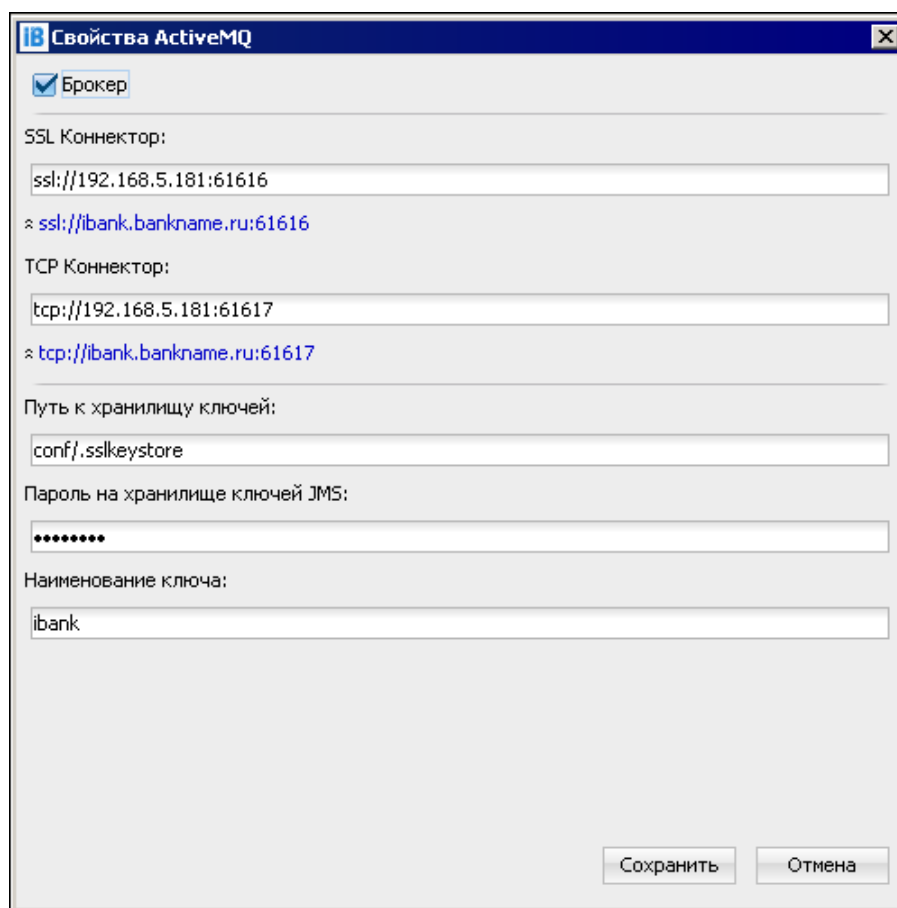


Рис. 24. Окно "Свойства ActiveMQ"

Признак **Брокер** предполагает выполнение сервером действий по обработке запросов генерации и преобразования уведомлений. Обеспечена возможность настройки брокера ActiveMQ для каждого сервера приложений многосерверной конфигурации. Допускается установка флага **Брокер** как для одного признанного брокером сервера, так и для каждого сервера многосерверной конфигурации.

В поле **SSL Коннектор** укажите IP-адрес или доменное имя сервера приложений и порт, на котором должна осуществляться работа брокера ActiveMQ.

В поле **Путь к хранилищу ключей** укажите относительный путь до хранилища секретных ключей SSL сервера приложений, например, `conf/.sslkeystore`

В поле **Пароль на хранилище ключей JMS** укажите пароль к хранилищу секретных ключей SSL сервера приложений.

В поле **Наименование ключа** укажите псевдоним (имя), под которым секретный ключ SSL сервера приложений хранится в хранилище.

Подробнее о SSL-сертификате см. раздел [Шаг 7](#).

При заполнении полей окна нажатием на значение ссылки **Пример** поле заполнится шаблонным значением. Не забудьте при этом указать истинные параметры сервера приложений.

Настройка реквизитов банка и филиалов

Настройка реквизитов банка и филиалов выполняется в разделе **Банки** (см. [рис. 25](#)). Список банков и филиалов необходимо формировать в соответствии с составом Лицензии.

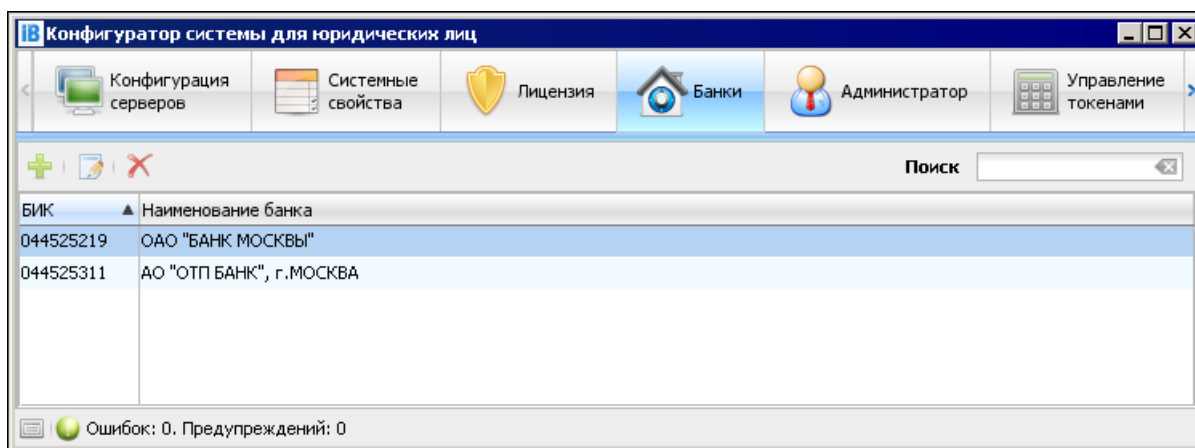


Рис. 25. Раздел "Банки" в модуле "Конфигуратор системы для юридических лиц"

Для добавления банка нажмите кнопку панели инструментов: откроется окно **Информация о банке** на закладке **Основная информация** (см. [рис. 26](#)).

На закладке **Основная информация** заполните обязательное поле **БИК**, тогда автоматически заполнятся поля **Наименование банка** и **Адрес банка** на русском языке. Эта информация берется из справочника БИК (см. раздел [Шаг 4](#)).

При необходимости заполните поля **ИНН** и **КПП**.

Заполните поле **Сокращенное наименование банка** на русском языке.

В паспортах сделки использование полного (поле **Наименование банка**) или краткого (поле **Сокращенное наименование банка**) наименования банка в документе зависит от свойства `documents.deal_passport.bank_name_type`

Заполните поле **SWIFT** (заполняется, если банк является участником системы SWIFT). При этом автоматически заполнятся поля **Наименование банка**, **Адрес банка** и **Город банка** на английском языке. Эта информация берется из справочника SWIFT (см. раздел [Шаг 5](#)). Если поле SWIFT оставить пустым, то поля **Наименование банка**, **Адрес банка** и **Город банка** на английском языке необходимо заполнить вручную.

Значения данных полей используются в документе "Заявление на перевод".

В поле **Наименование банка в сервисных сообщениях (SMS, MAC-токен BIFIT)** укажите значение, которое будет отображаться в уведомлениях, отправляемых клиенту посредством SMS и E-mail. Для отправки уведомлений на банковской стороне должен быть настроен сервис "SMS-Банк".

Клиент самостоятельно настраивает условия получения уведомлений и содержание информации в уведомлении. Клиент может получать уведомления, например, о движении средств по счету, о входе в систему и прочие (настраивается в разделе **Уведомления** клиентского модуля); уведомления об изменении статуса конкретного документа (настраивается на странице формы документа в клиентском модуле).

Значение поля **Наименование банка** используется в документах:

- Паспорт сделки по контракту;
- Паспорт сделки по кредитному договору;
- Заявление о переоформлении паспорта сделки;
- Заявление о закрытии паспорта сделки;
- Справка о валютных операциях;
- Справка о подтверждающих документах;
- Выписка.

The screenshot shows a window titled "iB Информация о банке" with three tabs: "Основная информация", "Контактная информация", and "Параметры банка". The "Основная информация" tab is active. It contains the following fields:

- BIK: 044525311
- SWIFT: MOSWRUMMXXX
- ИНН: 7708001614
- КПП: 997950001
- Section: **Поля для заполнения на русском языке**
- Наименование банка: АО "ОТП БАНК", г.МОСКВА
- Сокращенное наименование банка: "ОТП БАНК"
- Наименование банка в сервисных сообщениях (SMS, MAC-токен BIFIT): ОТП-Bank
- Адрес банка: г.МОСКВА
- Section: **Поля для заполнения на английском языке**
- Наименование банка: OPEN JOINT STOCK COMPANY "OTP BANK"
- Адрес банка: Город банка: MOSCOW
- 103802 MOSCOW KUZNETSKY MOST STREET 15

Buttons "Сохранить" and "Отмена" are located at the bottom right.

Рис. 26. Окно "Информация о банке". Закладка "Основная информация"

На закладке **Контактная информация** (см. рис. 27) укажите номера контактных телефонов банка, адрес web-сайта банка в Интернет и адрес электронной почты банка.

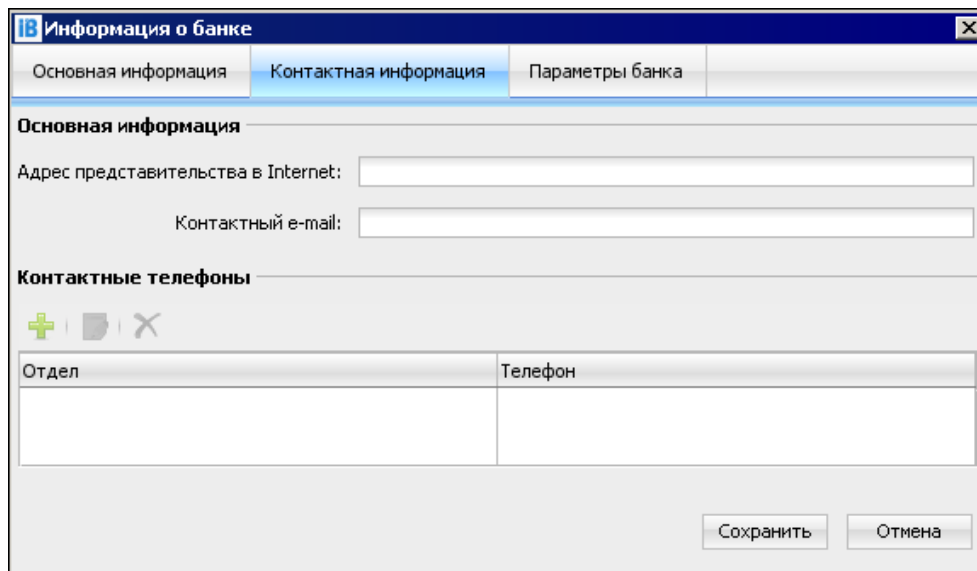



Рис. 27. Окно "Информация о банке". Закладка "Контактная информация"

Для ввода списка контактных телефонов банка нажмите на закладке кнопку  и в открывшемся окне **Контактный телефон отдела** (см. рис. 28) введите наименование отдела и номер телефона.

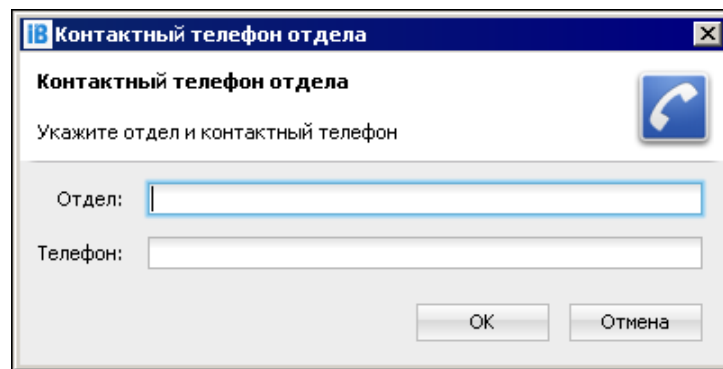



Рис. 28. Окно "Контактный телефон отдела"

На закладке **Параметры банка** задаются параметры, значения которых для данного банка могут отличаться от значений для всей системы. Для добавления параметров перейдите на закладку **Параметры банка** и нажмите кнопку  (см. рис. 29).

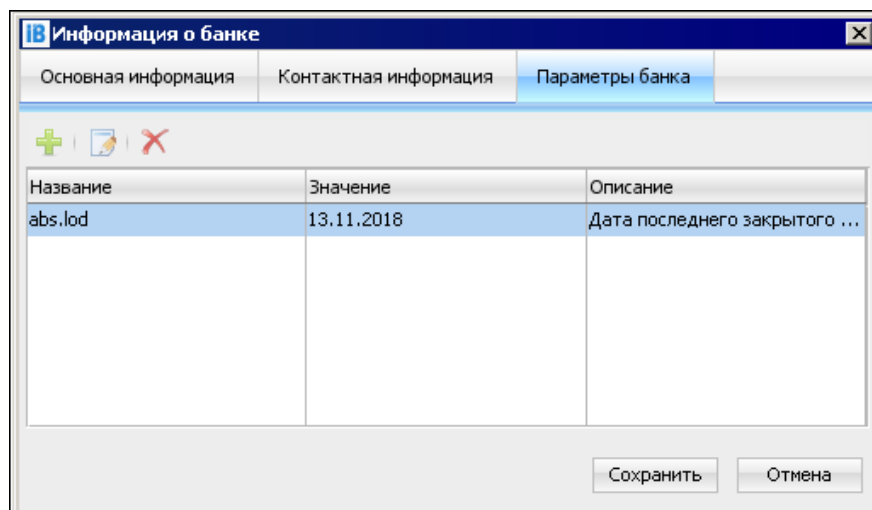




Рис. 29. Параметры банка

Сохраните внесенные изменения.

Для редактирования реквизитов банка выберите банк из списка и нажмите кнопку  панели инструментов. После внесения необходимых изменений сохраните результат.

Для удаления банка выберите нужный банк из списка и нажмите кнопку  панели инструментов.

Если в рамках одного экземпляра системы предполагается поддержка нескольких банков и их филиалов, то необходимо ввести по каждому из банков аналогичную информацию. Зарегистрированные в системе "iBank для Бизнеса" банки должны быть указаны в Лицензии.

Назначение главного администратора

Назначение главного администратора выполняется в модуле "Конфигуратор системы для юридических лиц" в разделе **Администратор** (см. [рис. 30](#)).

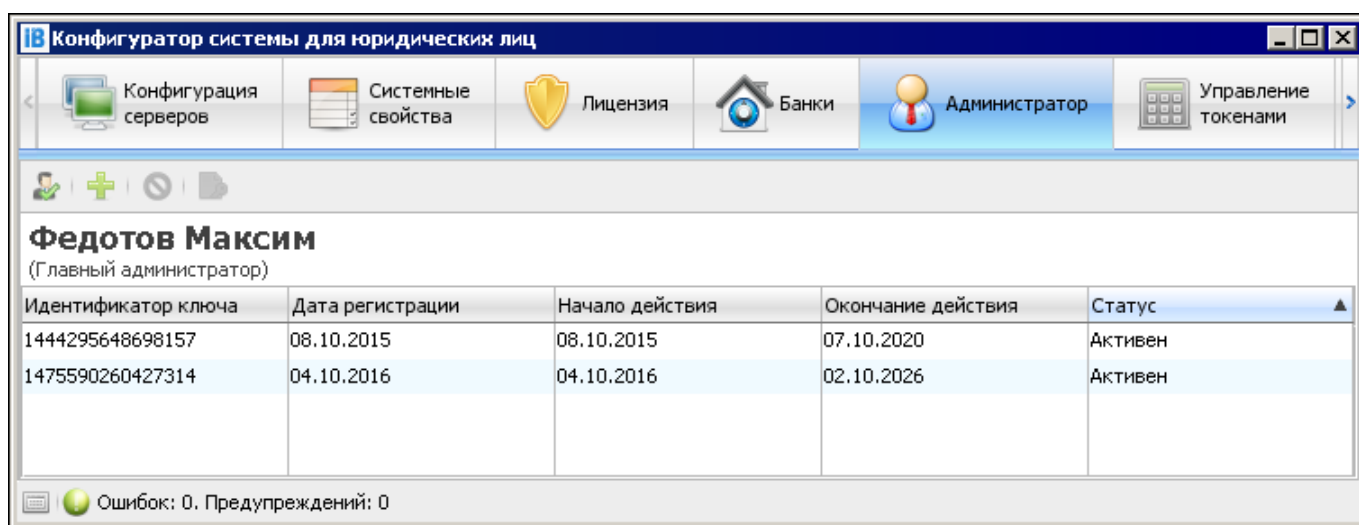


Рис. 30. Раздел "Администратор"

Главный администратор осуществляет управление клиентами и сотрудниками головного банка, а также регистрирует в системе администраторов филиалов.


Главный администратор и администраторы филиалов используют в своей работе единый модуль "Администратор банка/филиала".

Разграничение прав и функций по управлению клиентами и банковскими сотрудниками выполняется при входе в модуль в соответствии с ключами ЭП, с которыми выполняется аутентификация в системе.

Внимание!

В системе может быть только один пользователь с ролью "главный администратор"!

Перед назначением главного администратора, сотруднику, который будет исполнять эти функции, необходимо через модуль "Регистратор банковских сотрудников" зарегистрироваться в системе и сгенерировать ключ ЭП, который впоследствии он будет использовать для аутентификации и работы в системе.

Для назначения главного администратора нажмите кнопку  панели инструментов раздела: откроется окно **Назначение главного администратора** со списком новых зарегистрированных в системе банковских сотрудников (см. [рис. 31](#)).

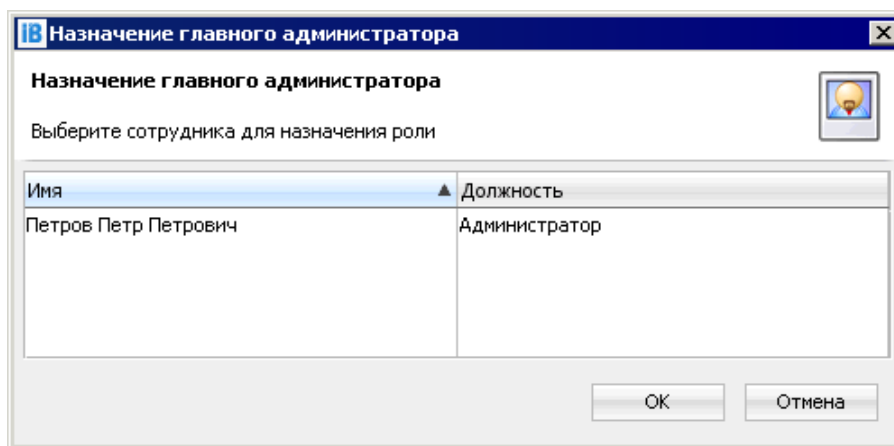


Рис. 31. Окно "Назначение главного администратора"

Выберите из списка необходимого сотрудника для назначения роли и нажмите кнопку **ОК**.

Зарегистрированный один раз ключ ЭП для сотрудника с ролью "главный администратор" не может быть использован повторно, это означает что при назначении главного администратора всегда необходимо использовать новый ключ ЭП.

Таким образом, последовательность действий по регистрации и назначению администраторов будет следующей:

1. В модуле "Регистратор банковских сотрудников" выполняется регистрация и генерация ключа ЭП для главного администратора.
2. В модуле "Конфигуратор системы для юридических лиц" выполняется регистрация ключа ЭП главного администратора.
3. В модуле "Регистратор банковских сотрудников" выполняется регистрация и генерация ключа ЭП для администратора филиала.
4. В модуле "Администратор банка/филиала" главный администратор выполняет регистрацию ключа ЭП администратора филиала.

Шаг 9. Запуск и остановка сервера приложений "iBank для Бизнеса"

Индивидуальная настройка Java для сервера приложений

Если вы **не** используете для Java переменных системного окружения, то раскомментируйте и установите значение переменной `JAVA_HOME` в командном файле `$SERVER_ROOT/bin/setvars.sh`, где `$SERVER_ROOT` — каталог с установленным сервером приложений.

Примечание:

Перед первым запуском сервера приложений проверьте:

1. настройки Java;
2. наличие установленной Лицензии на необходимую конфигурацию банковской компоненты и необходимое количество клиентов (см. раздел [Установка Лицензии](#));
3. наличие конфигурационного файла `connection.xml` в каталоге развернутого сервера приложений — `$SERVER_ROOT/conf`;
4. наличие SSL-сертификата (SSL-хранилище должно находиться в каталоге развернутого сервера приложений — `$SERVER_ROOT/conf`).

Запуск сервера приложений выполняется запуском командного файла `$SERVER_ROOT/bin/startup.sh` с аргументом `run` или `start`, где

`run` — консоль сервера приложений будет отображена в текущем окне;

`start` — консоль сервера приложений будет отображена в новом окне.

Все настройки конфигурации сервера приложений хранятся в базе данных. При каждом запуске сервера его конфигурация устанавливается согласно сохраненной в БД.

Остановка сервера приложений выполняется запуском командного файла `$SERVER_ROOT/bin/shutdown.sh`.

Дополнительные параметры запуска сервера приложений (могут понадобиться в процессе эксплуатации системы):

- `startup loadoff run` — запуск сервера приложений без обновления его конфигурации согласно сохраненной в БД;
- `startup backupoff run` — запуск сервера приложений без предварительного создания его резервной копии (по умолчанию резервное копирование файлов сервера приложений выполняется в каталог `$SERVER_ROOT/backups`);
- `startup verifyoff run` — запуск сервера приложений без проверки электронной подписи под конфигурацией сервера (подробнее об электронной подписи конфигурации см. в руководстве модуля "Конфигуратор системы для юридических лиц").

Генерация ключей шифрования сервера приложений "iBank для Бизнеса"

При каждом запуске сервера приложений выполняется проверка на наличие сеансовых ключей шифрования сервера приложений. Эти ключи необходимы при взаимодействии клиентских java-приложений ("Корпоративный автоклиент" и "Тикер для корпоративных клиентов") с сервером приложений и предназначены для шифрования и контроля целостности передаваемой информации. Сеансовые ключи загружаются к клиентам через HTTPS-протокол на этапе загрузки java-приложений.

Шаг 10. Формирование дистрибутивов клиентских модулей

Формирование дистрибутивов клиентских модулей выполняется при помощи утилиты `$SERVER_ROOT\bin\make_dist.bat`. При помощи утилиты можно сгенерировать дистрибутивы:

- Администратор банка/ филиала;
- Тикер для операционистов;
- Тикер для корпоративных клиентов;
- Корпоративный автоклиент.

Перед запуском утилиты выполните настройки:

- **Настройка точек доступа для клиентских модулей**

Настройка адреса точек доступа для подключения клиентских модулей выполняется через свойства и описана в разделе [Настройка клиентских приложений системы](#).

- **Настройка наименования банка в заголовках клиентских приложений и в ярлыках для запуска клиентских приложений**

Выполните настройку наименования в свойстве `company.client_app.bank_name` в разделе **Системные свойства** модуля "Конфигуратор системы для юридических лиц". Действие является обязательным для создания дистрибутива.

Значение используется:

- в названии ярлыка для запуска модулей "Тикер для операционистов" и "Тикер для корпоративных клиентов" на стороне банковского сотрудника и клиента соответственно;
- в заголовке окна пользовательского java-приложения;
- в заголовке закладки браузера (для web-приложений).

- **Включение СКЗИ в клиентский дистрибутив корпоративного автоклиента**

Отредактируйте значение переменной `INCLUDE_CRYPTO` в командном файле `$SERVER_ROOT\bin\setvars.bat`. Допустимые значения: `yes`, `no`. Значение по умолчанию: `yes`.

Дистрибутив СКЗИ должен быть получен у сотрудников компании "БИФИТ" и размещен в каталоге `$SERVER_ROOT\lib\native` (см. раздел [Настройка СКЗИ](#)).

Для генерации дистрибутива с включенными криптобиблиотеками, отредактируйте значение переменной `CRYPTO_PATH` `$SERVER_ROOT\bin\setvars.bat`, указав полный путь к криптобиблиотекам.

- **Создание дистрибутива Тикер для операционистов и Корпоративный автоклиент со встроенным SSL-сертификатом (используется для самозаверенных сертификатов)**

Отредактируйте значение переменной `CERT_PATH` в командном файле `$SERVER_ROOT\bin\setvars.bat`, указав путь до сертификата. Например, `c:\iBank\server\CaCert2048.der`.

Запустите утилиту формирования дистрибутивов `$SERVER_ROOT\bin\make_dist.bat`.

В результате работы утилиты будут сформированы дистрибутивы:

<code>autoclient.zip</code>	архив дистрибутива Корпоративный автоклиент
<code>ticker-corporate.exe</code>	дистрибутив Тикер для корпоративных клиентов
<code>ticker-operator.exe</code>	дистрибутив Тикер для операционистов
<code>Administrator.exe</code> , <code>Administrator.tar.bz2</code>	дистрибутив Администратора банка/ филиала для Windows и для Unix

Файлы дистрибутивов будут сформированы в каталоги:

- `$SERVER_ROOT\webapps-local\ROOT`
 - Администратора банка/ филиала;
 - Тикер для операционистов;
- `$SERVER_ROOT\webapps-public\ROOT`
 - Корпоративный автоклиент;
 - Тикер для корпоративных клиентов.

Шаг 11. Формирование программы для подготовки рабочего места клиента

Для упрощения подготовки рабочего места корпоративного клиента используется специализированная программа (далее инсталлятор) для установки ПО, необходимого для работы в модуле "Интернет-Банк для Бизнеса" и модуле "Центр финансового контроля" (ЦФК):

- VIFIT Signer;
- Файловые криптобиблиотеки, если используется файловое хранилище ключей.

Формирование инсталлятора выполняется при помощи утилиты `$SERVER_ROOT/bin/create_web_installer.sh`

Внимание!

Инсталлятор формируется только для клиентов, использующих ОС Windows.

Перед запуском утилиты `$SERVER_ROOT/bin/create_web_installer.sh` в исполняемом файле `$SERVER_ROOT/bin/setvars.sh` выполните настройки:

- **Настройка наименования инсталлятора**

Укажите наименование инсталлятора, отредактировав значение переменной `INST_NAME`. Действие является обязательным.

Наименование инсталлятора обязательно для заполнения.

Пример:

```
SET INST_NAME=iBank
```

- **Настройка иконки инсталлятора**

При необходимости укажите путь к изображению, которое будет использоваться в качестве иконки инсталлятора, отредактировав значение переменной `INST_IMG_ICON`

Параметры изображения: размер — 32x32 px; формат — ico.

Пример:

```
SET INST_IMG_ICON="/home/username/resources/images/favicon.ico"
```

- **Настройка отображения боковой панели интерфейса инсталлятора**

При необходимости укажите путь к изображению, которое будет отображаться в боковой панели окна инсталлятора, отредактировав значение переменной `INST_IMG_SIDEBAR`

Параметры изображения: размер — 164x314 px; формат — bmp.

Пример:

```
SET INST_IMG_SIDEBAR="/home/username/resources/images/vertical.bmp"
```

- **Включение криптобиблиотек в инсталлятор**

Если банк планирует предоставлять клиентам возможность использования файловых хранилищ ключей, то укажите пути к каталогам, в которых содержатся файлы криптобиблиотек для добавления в дистрибутив инсталлятора, отредактировав значение переменной `INST_LIBRARIES_32BIT`. Пути указываются для каждого файла отдельно и разделяются пробелом.

Пример:

```
SET INST_LIBRARIES_32BIT="/home/username/resources/lib/ccom.dll /home/username/resources/lib/ccom.dll.sig"
```

Запустите исполняемый файл `$SERVER_ROOT/bin/create_web_installer.sh`.

В результате работы утилиты в каталоге `$SERVER_ROOT/webapps-public/ROOT/` будет сформирован файл дистрибутива инсталлятора `web_installer.exe`.

Соответствие настройки утилиты интерфейсу инсталлятора приведено на [рис. 32](#).

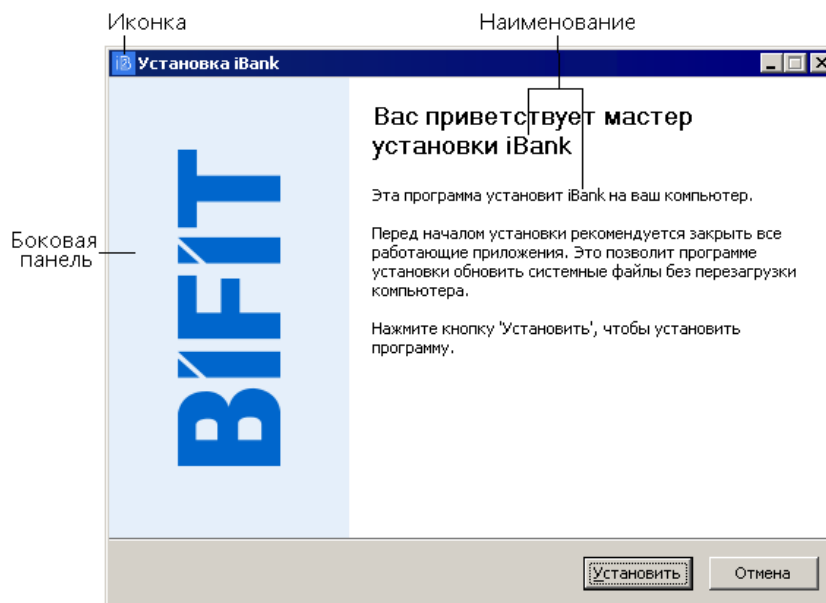


Рис. 32. Интерфейс инсталлятора

Отображение клиентам ссылки для скачивания дистрибутива инсталлятора регулируется системным свойством `corporate.web_installer.enable` в модуле "Конфигуратор системы для юридических лиц".

Ссылка на дистрибутив инсталлятора отображается клиентам на странице входа в модуль при выполнении следующих условий (см. [рис. 33](#)):

- На компьютере клиента не установлен плагин BIFIT Signer;
- Клиент является пользователем ОС Windows;
- Свойство `corporate.web_installer.enable=true`;
- Инсталлятор сформирован в `$SERVER_ROOT/webapps-public/ROOT/web_installer.exe`

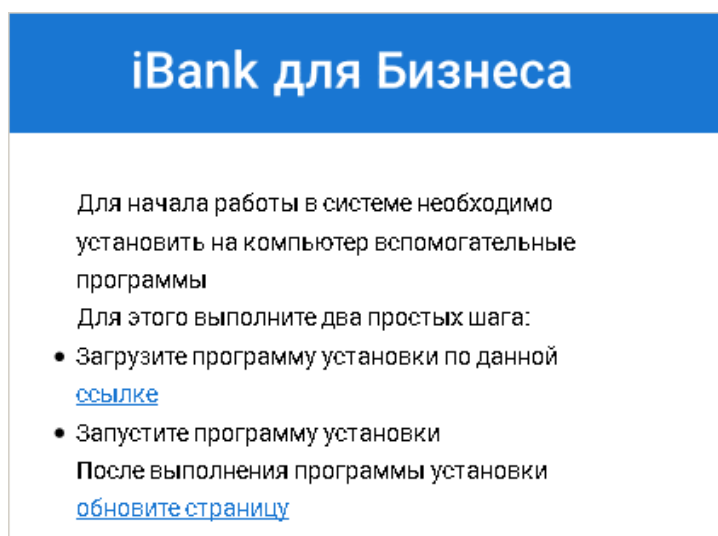


Рис. 33. Страница входа в модуль "Интернет-Банк для Бизнеса"

Шаг 12. Вход в модули системы

Для контроля правильности установки системы и конфигурации сервера приложений выполните проверку доступности клиентских модулей.

Банковские сотрудники

Для входа в свои модули банковские сотрудники в браузере используют ссылку вида `https://iBank для Бизнеса.bankname.ru:9443/index.html` (адрес и порт доменного имени сервера приложений настраиваются в разделе [Настройка клиентских приложений системы](#)).

Внешний вид страницы представлен на [рис. 34](#) (шаблон страницы находится в каталоге `$SERVER_ROOT/webapps-local/ROOT`).

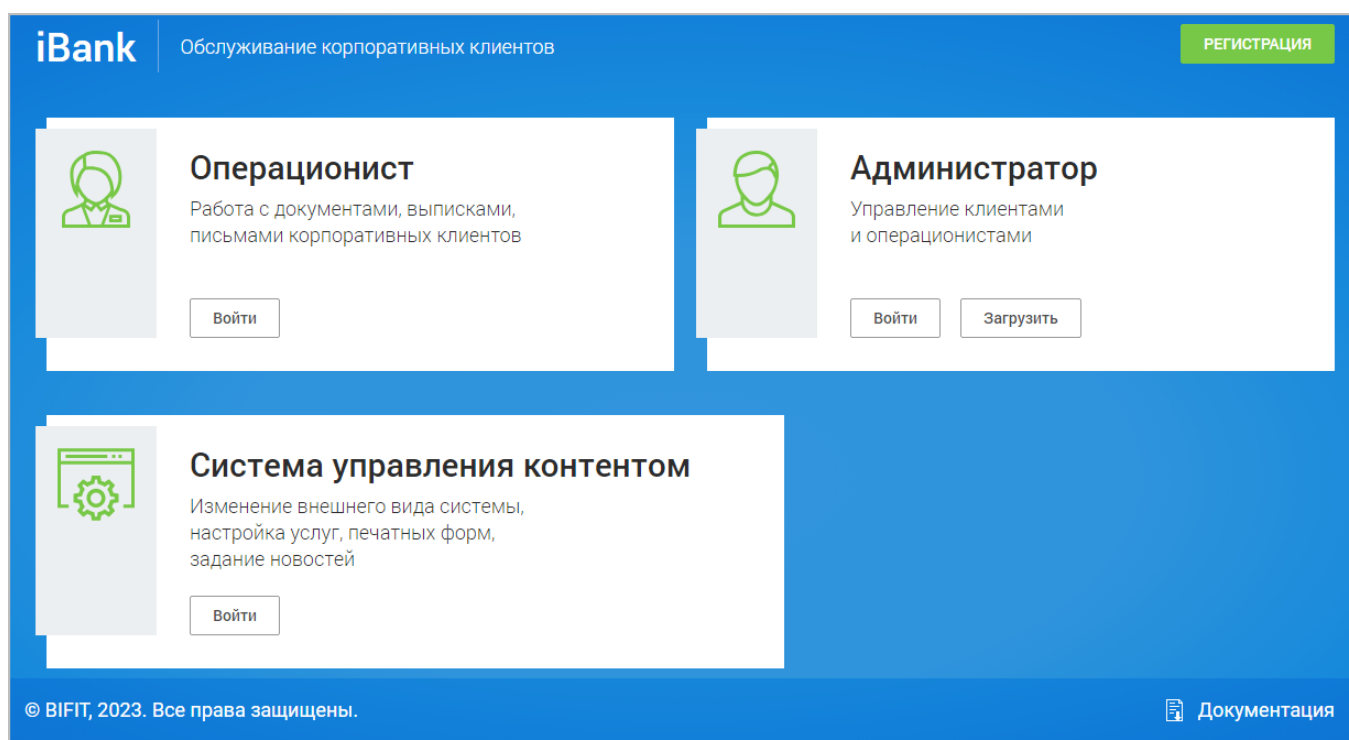


Рис. 34. Стартовая страница банковских сотрудников

Корпоративные клиенты банка

Для входа в свои модули клиенты банка в браузере используют ссылку вида `https://iBank для Бизнеса.bankname.ru/index.html` (адрес и порт доменного имени сервера приложений настраиваются в разделе [Настройка клиентских приложений системы](#)).

Внешний вид страницы представлен на [рис. 35](#) (шаблон страницы находится в каталоге `$SERVER_ROOT/webapps-public/ROOT`).

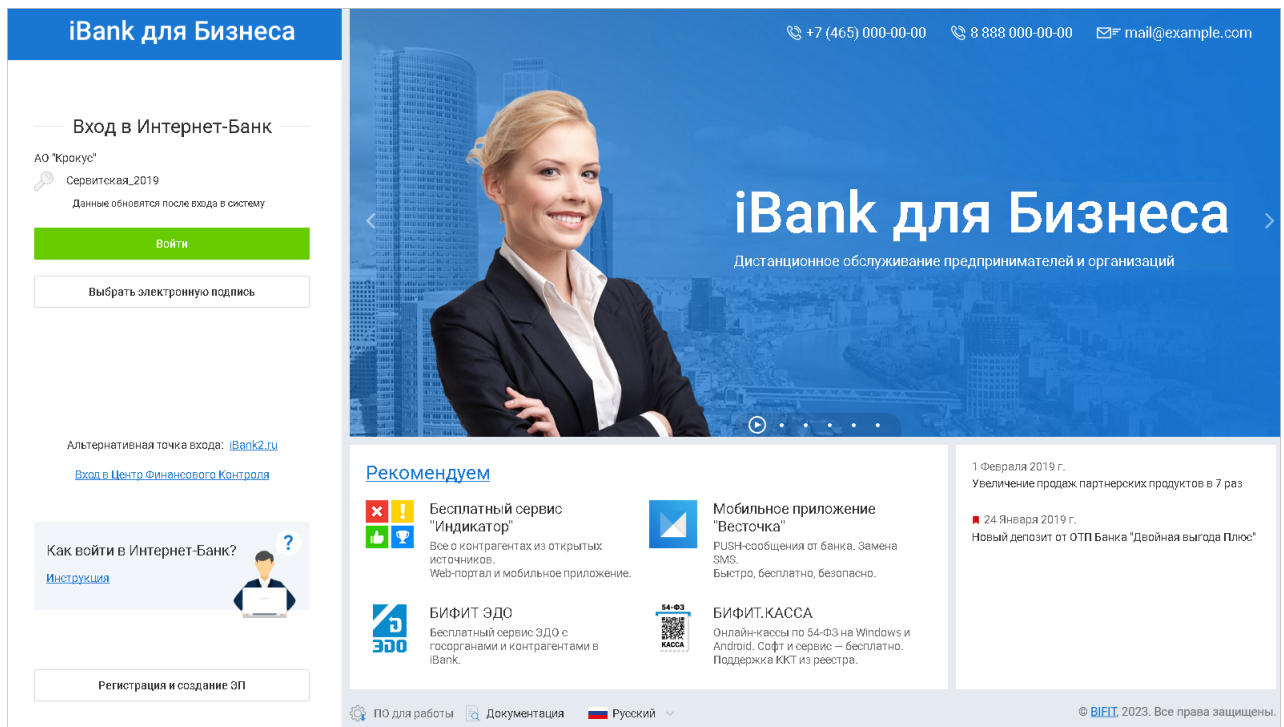


Рис. 35. Стартовая страница клиентов банка

Шаг 13. Загрузка производственного календаря

Данные календаря праздничных дней и рабочих дней, приходящихся на выходные, сохраняются в БД в таблице CALENDAR.

Данные из таблицы CALENDAR обеспечивают корректную работу:

- документа "Выписка по расписанию";
- проверки лимитов после получения последней подписи под документами **Платежное поручение** и **Заявление на перевод**.

Таблицу CALENDAR необходимо заполнять по годам. Для операционного года таблица считается заполненной, если она содержит хотя бы одну запись для даты из данного года.

Загрузка данных производственного календаря выполняется с помощью утилиты `$SYSCON_ROOT/bin/load_holidays_calendar.sh`.

Перед запуском утилиты:

- Если график праздничных и рабочих дней, приходящихся на выходные, в вашей организации отличается от соответствующего общероссийского календаря, отредактируйте данные в файле `$SYSCON_ROOT/refs/holidays_calendar/holidays_calendar.json`:
 - в секции "year" указывается год, для которого задают график праздничных и рабочих дней. Секции с годами должны быть разделены между собой символом ",";
 - в блоке "holidays" для каждого года указываются даты праздничных дней;
 - в блоке "workdays" для каждого года указываются даты рабочих дней, приходящихся на выходные.

Пример файла `holidays_calendar.json`:

```
[
  {
    "year":2021,
    "holidays": [
      "01.01.2021",
      "04.01.2021",
      "05.01.2021"
    ],
    "workdays": [
      "20.02.2021"
    ]
  },
  {
    "year":2022,
    "holidays": [
      "03.01.2022",
      "04.01.2022",
      "05.01.2022"
    ],
    "workdays": [
      "05.03.2022"
    ]
  }
]
```

По умолчанию файл `$SYSCON_ROOT/refs/holidays_calendar/holidays_calendar.json` содержит производственные календари с 2012 по 2022 год, с учетом общероссийских государственных праздников.

- Если файл `holidays_calendar.json` с данными для загрузки располагается в каталоге, отличном от `$SYSCON_ROOT/refs/holidays_calendar`, укажите путь к требуемому каталогу в исполняемом файле `$SYSCON_ROOT/bin/setvars.bat`, отредактировав строку `set REFS_HOLIDAYS_CALENDAR=`.

Запуск утилиты для обновления производственного календаря может осуществляться в двух режимах:

- с перезаписью существующих данных (запуск с параметром `true`);
- без перезаписи существующих данных (запуск без параметров).

Отчет о результатах загрузки календаря в БД системы "iBank для Бизнеса" сохраняется в файл `$SYSCON_ROOT/logs/load_holidays_calendar.log`.

Приложение 1. Настройка СКЗИ

Для криптографической защиты информации в систему "iBank для Бизнеса" встроена поддержка сертифицированной ФСБ РФ многоплатформенной криптобиблиотеки СКЗИ "Крипто-КОМ 3.5".

Криптобиблиотека реализует криптографические функции защиты информации и электронной подписи, соответствуют требованиям ФСБ России к средствам криптографической защиты информации класса КС1, КС2 и обеспечивает конфиденциальность и целостность передаваемой и хранимой информации, аутентификацию пользователей.

Криптобиблиотека распространяется на основании лицензионного договора компании "БИФИТ" с разработчиком СКЗИ. Для использования клиентом банка СКЗИ необходимо наличие криптобиблиотеки на стороне клиента.

Криптобиблиотека не входит в состав дистрибутива клиентской части системы "iBank для Бизнеса". Клиенты должны получить файлы криптобиблиотеки в банке и самостоятельно установить ее на компьютеры, с которых они будут осуществлять свою работу с системой "iBank для Бизнеса" (см. раздел [Установка СКЗИ "Крипто-КОМ 3.5" на стороне клиента/сервера](#)).

Настройка типа криптографии и установка криптобиблиотеки состоит из нескольких этапов.

Выбор типа криптографии, используемой на стороне сервера приложений

Для использования криптографии на сервере приложений перейдите в раздел **Системные свойства** модуля "Конфигуратор системы для юридических лиц" (см. [рис. 36](#)).

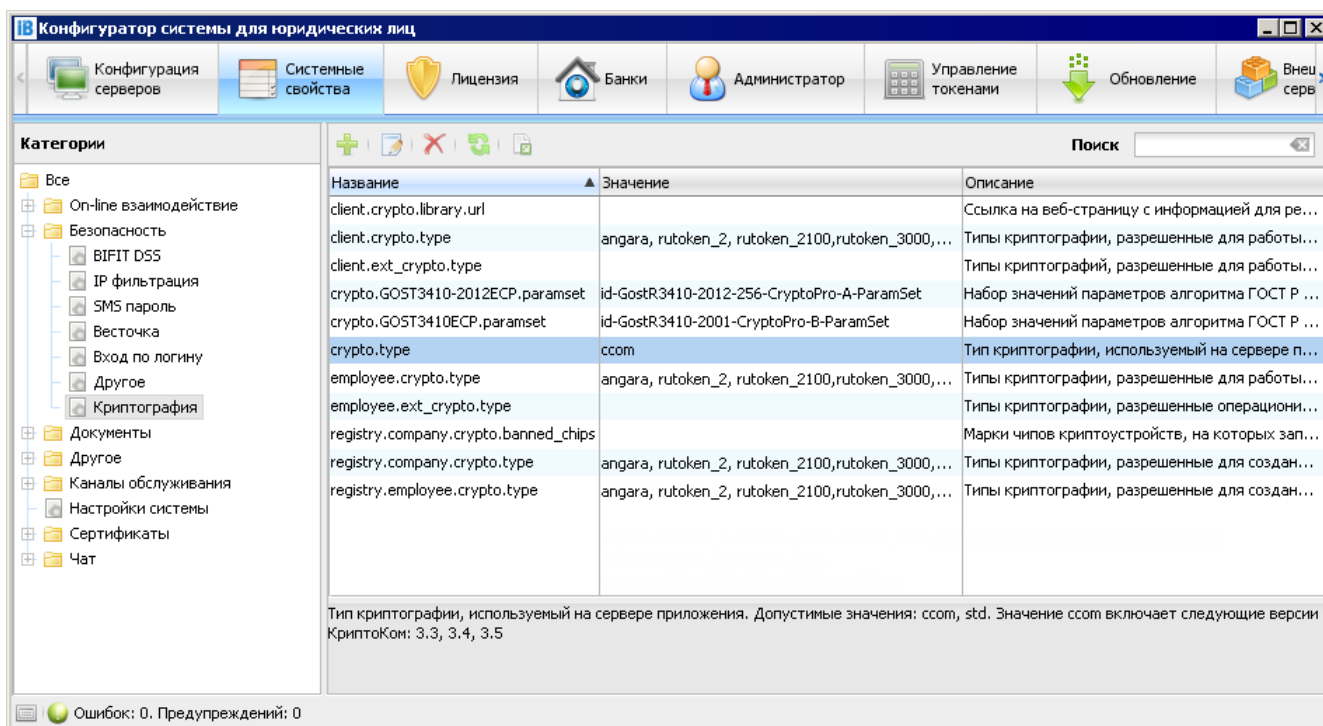



Рис. 36. Раздел "Системные свойства" модуль "Конфигуратор системы для юридических лиц"

В списке системных свойств перейдите в категорию **Безопасность/Криптография** и выберите свойство `crypto.type`. Для редактирования нажмите кнопку  панели инструментов.

В отобразившемся окне **Системное свойство** (см. [рис. 37](#)), в поле **Значение** укажите только одно значение. Для использования СКЗИ "Крипто-КОМ 3.5" укажите служебное название `ccom`

Сохраните внесенные изменения.

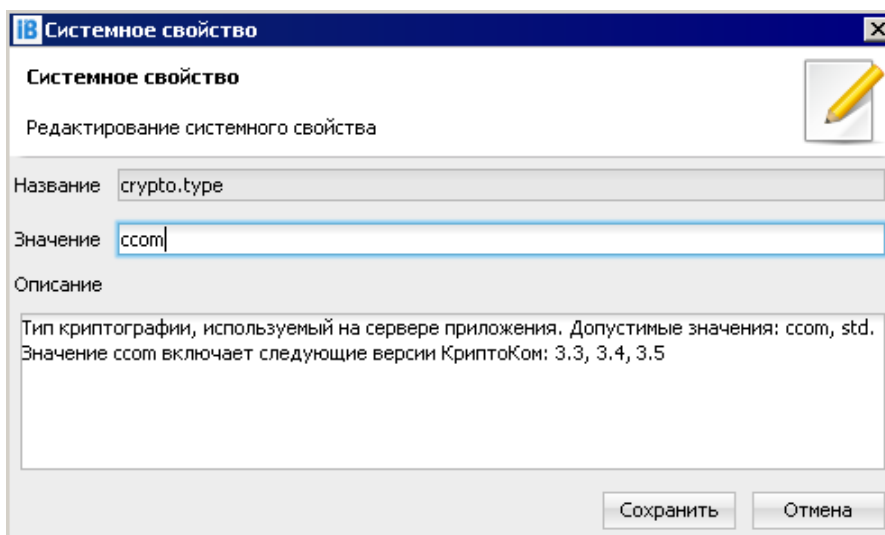



Рис. 37. Окно "Системное свойство"

Выбор типов криптографии, используемых на стороне клиента

Для определения типов криптографии, которые можно использовать на стороне клиента, перейдите в раздел **Системные свойства** модуля "Конфигуратор системы для юридических лиц".

В списке системных свойств перейдите в категорию **Безопасность/Криптография** и выберите свойство `client.crypto.type`. Для редактирования нажмите кнопку  панели инструментов.

В отобразившемся окне **Редактирование свойства** (см. рис. 38), в поле **Значение** для использования СКЗИ "Крипто-КОМ 3.5" укажите служебное название `ccom35`.

Сохраните внесенные изменения.

Значение свойства и настройки криптографии в файле `$SERVER_ROOT/webapps-public/ROOT/params.js` должны совпадать. После изменения свойства необходимо пересохранить конфигурацию сервера приложений для автоматической синхронизации файла `params.js`

Если на стороне клиента библиотека "Крипто КОМ 3.5" отсутствует, клиенту отобразится сообщение о необходимости установить ее.

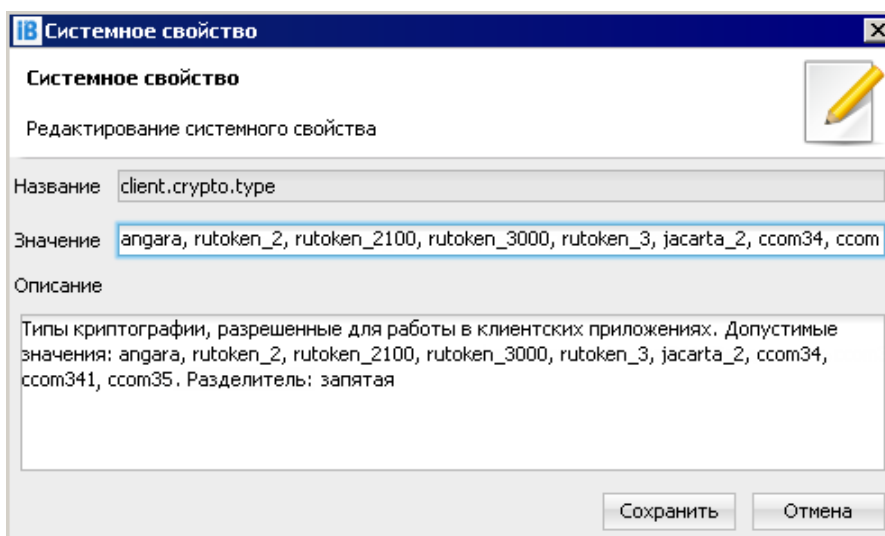


Рис. 38. Окно "Системное свойство"

Установка СКЗИ "Крипто-КОМ 3.5" на стороне клиента/ сервера приложений

СКЗИ "Крипто-КОМ 3.5" устанавливается путем размещения файлов криптобиблиотеки в среде пользовательской ОС. В зависимости от типа используемой ОС и ее разрядности выполните следующее:

- **Linux x64**

— в каталог `/usr/lib` поместите файлы 64-битной криптобиблиотеки `libccom.so`, `libccom.so.sig`, `libsctrng.so`.

- **Linux x86**

— в каталог `/usr/lib` поместите файлы 32-битной криптобиблиотеки `libccom.so`, `libccom.so.sig`, `libsctrng.so`.

- **Windows x64**

— в каталог `C:\Windows\System32` поместите файлы 64-битной криптобиблиотеки `ccom.dll`, `ccom.dll.sig`, `sctrng.dll`.

— в каталог `C:\Windows\SysWOW64` поместите файлы 32-битной криптобиблиотеки `ccom.dll`, `ccom.dll.sig`, `sctrng.dll`.

- **Windows x86**

— в каталог `C:\Windows\System32` поместите файлы 32-битной криптобиблиотеки `ccom.dll`, `ccom.dll.sig`, `sctrng.dll`.

Приложение 2. Рекомендации по размещению компонент системы "iBank для Бизнеса"

Архитектурно система "iBank для Бизнеса" может состоять из сервера приложений со встроенным web-сервером, сервера баз данных и модуля интеграции с АБС.

С точки зрения безопасности рекомендуется располагать сервер приложений и сервер баз данных в демилитаризованной зоне (DMZ), а модуль интеграции — в локальной сети банка. Это дает возможность запретить установку соединения из DMZ в локальную сеть банка.

Необходимо обеспечить отказоустойчивость системы. Выход из строя сервера системы "iBank для Бизнеса" влечет за собой недоступность услуг электронного банкинга для клиентов.

Все проекты по внедрению системы электронного банкинга "iBank для Бизнеса" должны содержать в себе "горячее" резервирование серверов приложений, серверов СУБД и каналов доступа в Интернет. В идеале конфигурация системы должна содержать в себе 2 сервера приложений, 2 канала, которые используются обоими серверами одновременно, и средства резервирования СУБД.

Рекомендуемая схема размещения компонент системы "iBank для Бизнеса" в банке представлена на рис. 39.

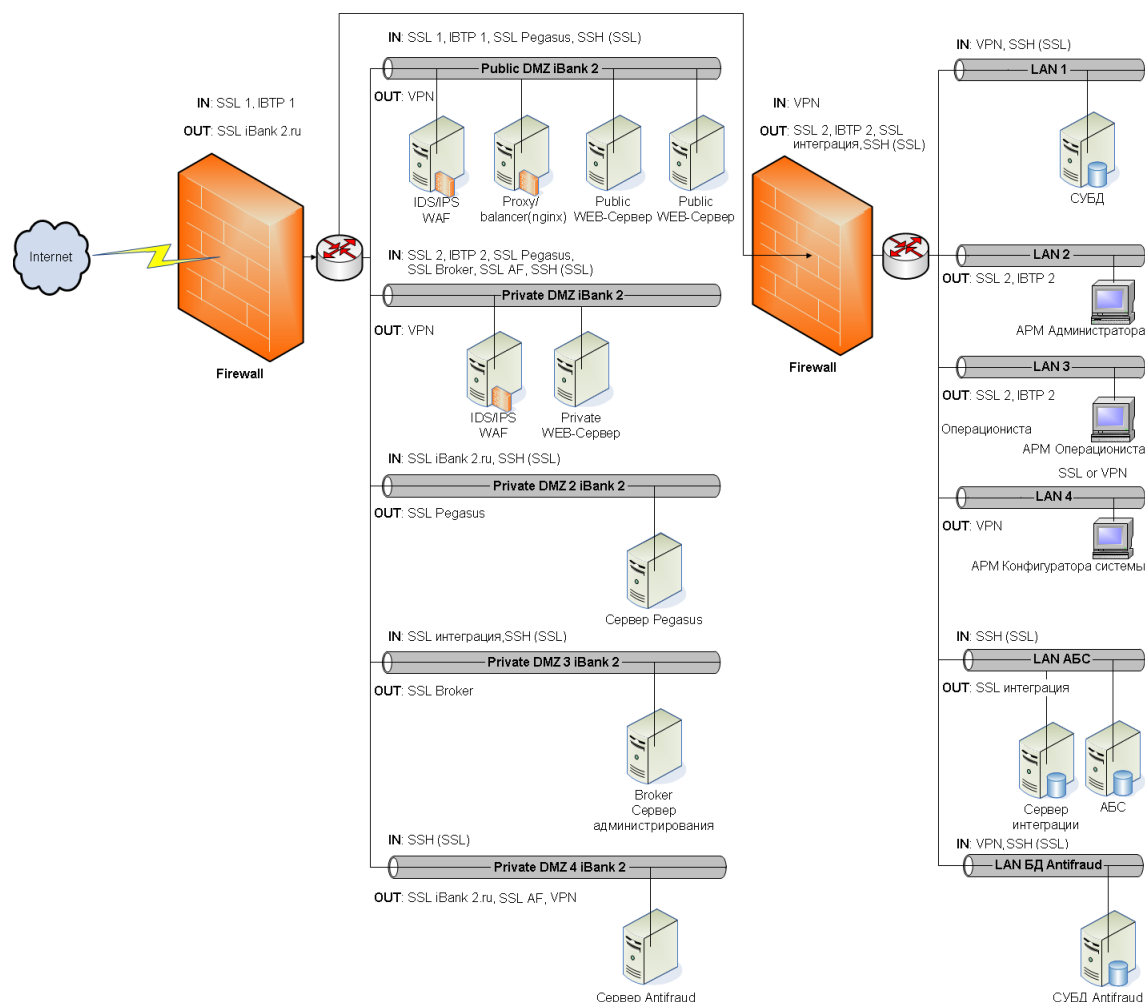


Рис. 39. Схема размещения компонент системы "iBank для Бизнеса" в банке

Приложение 3. Рекомендации по техническому обеспечению

Примечание:

При выборе конфигурации следует учитывать не только текущее количество клиентов и документооборот, но и рост в перспективе на 5 лет (т.е. указанное количество клиентов должно быть ожидаемым количеством клиентов через 5 лет).

Для количества клиентов до 200

- Единый сервер для сервера приложений системы "iBank для Бизнеса" и СУБД:
 - 1 x Xeon E3-1270
 - 8 GB RAM
 - HDD 4 x 500Gb SAS
 - RAID 10
- Сервер для модуля интеграции:
 - 1 x Xeon E3-1220
 - 4 GB RAM
 - HDD 1 x 300Gb SAS
- Виртуальные машины соответствующей конфигурации.

Для количества клиентов от 200 до 500 и документооборота до 1 000 документов в день

- Единый сервер для сервера приложений системы "iBank для Бизнеса" и СУБД:
 - 2 x Xeon E5-2407
 - 12 GB RAM
 - HDD 4 x 500Gb SAS
 - RAID 10
- Сервер для модуля интеграции:
 - 1 x Xeon E3-1220
 - 8 GB RAM
 - HDD 1 x 300Gb SAS
- Виртуальные машины соответствующей конфигурации.

Для количества клиентов от 500 до 1000 и документооборота до 2 000 документов в день

Для данного количества клиентов и документооборота сервер приложений системы "iBank для Бизнеса" и сервер СУБД можно развернуть как на одной машине, так и на отдельных:

- Единый сервер для сервера приложений системы "iBank для Бизнеса" и СУБД:
 - 2 x Xeon E5-2643
 - 24 GB RAM
 - HDD 4 x 500Gb SAS
 - RAID 10
- Если планируется использовать отдельный сервер для сервера приложений системы "iBank для Бизнеса" и отдельный сервер для СУБД, рекомендуется два сервера следующей конфигурации:

- 2 x Xeon E5-2407
- 12 GB RAM
- HDD 4 x 500Gb SAS
- RAID 10
- В обоих вариантах для сервера модуля интеграции может использоваться следующая конфигурация:
 - 2 x Xeon E5-2403
 - 12 GB RAM
 - HDD 1 x 300Gb SAS
- Виртуальные машины соответствующей конфигурации.

Для количества клиентов от 1000 до 5000 и документообороте до 10 000 документов в день

- Сервер для сервера приложений:
 - 2 x Xeon E5-2670
 - 32 GB RAM
 - HDD 4 x 500Gb SAS
 - RAID 10
- Сервер для СУБД:
 - 2 x Xeon E5-2670
 - 32 GB RAM
 - HDD 4 x 500Gb SAS
 - RAID 10
- Сервер модуля интеграции:
 - 2 x Xeon E5-2403
 - 12 GB RAM
 - HDD 1 x 300Gb SAS

Для количества клиентов свыше 5000 конфигурацию необходимо подбирать отдельно.

Приложение 4. Список логов сервера приложений

Название файла лога	Описание
access.log	Лог всех запросов сервера (на все порты, перечисленные в \$SERVER_ROOT/conf/server.xml). Количество выводимой информации настраивается в \$SERVER_ROOT/conf/server.xml
admin.log	Лог работы модуля "Администратор банка/филиала"
antifraud.log	Лог работы модуля "Fraud-мониторинг для корпоративных клиентов"
api.log	Лог для записи отладочной информации из модуля \$SERVER_ROOT/webapps-public/api.war
auth.log	Лог для записи отладочной информации при взаимодействии с внешними системами
auth-client.log	Лог внешнего модуля аутентификации
autoclient.log	Лог работы модуля "Корпоративный автоклиент"
cfc.log	Лог работы модуля "Центр финансового контроля"
cms.log	Лог работы модуля "Система управления контентом (CMS)"
detector.log	Лог модуля "Детектор угроз"
directbank1c.log	Лог модуля "iBank для 1С"
hibernate.log	Лог работы модуля Hibernate, позволяющего абстрагироваться от особенностей конкретной СУБД, используется для запросов к СУБД в модуле "Интернет-Банк для Бизнеса"
ibank2web.log	Лог работы модуля "Интернет-Банк для Бизнеса"
ipfilter.log	Лог работы IP-фильтра
jms-online.log	Лог Jms-online
launcher.log	Лог запуска сервера приложений
login_auth_confirm.log	Лог для записи информации по настройке входа по логину в "Интернет-Банк для Бизнеса"
mobile_api.log	Лог для записи отладочной информации из модуля \$SERVER_ROOT/webapps-public/mobile_api.war
operator2web.log	Лог работы модуля "Операционист"
pegasus.log	Лог работы модуля "Шлюз рассылки уведомлений"
plugin1c.log	Лог работы клиентов через плагин "iBank для 1С:Предприятия"
registry.log	Лог работы модуля "Регистратор"
server-iBank.log	Лог, в котором отражается состав лицензии на ПО компании "БИФИТ"
ticker.log	Лог работы модуля "Тикер для корпоративных клиентов"
ticker-operator.log	Лог работы модуля "Тикер для операционистов"
tomcat.log	Лог запуска и работы сервера приложений
zclient.log	Лог работы сервиса предварительной регистрации "Нулевой клиент"
zeroclient.log	Лог работы сервиса "Нулевой клиент" при полнофункциональной регистрации клиента

Приложение 5. Информация о совместимости и обновлении системы

Информация о совместимости

Необходимо соблюдать совместимость версий:

- Системы «iBank для Бизнеса»;
- Платформы интеграции;
- Мобильных приложений.

Для операционной системы iOS работоспособность приложений «Мобильный Банк для Бизнеса» обеспечена для последних трех версий ОС.

Загрузка, установка, обновление

Система «iBank для Бизнеса» распространяется через службу внедрения и сопровождения компании «БИФИТ». Доступны:

- Дистрибутив для первоначальной установки;
- Дистрибутив для последующих обновлений.

Количество версий, с которых можно обновить систему, ограничено 5 предыдущими сборками. Если установлена более ранняя версия, необходимо установить промежуточную версию.

Дополнительные модули:

- Платформа интеграции;
- Адаптеры для платформы интеграции с АБС и внешними системами.

Важно:

- Перед проведением обновления обязательно сделайте резервную копию сервера приложений и базы данных;
- Установка обновления на промышленный контур должна осуществляться только после проверки обновления на тестовом контуре.

Порядок обновления сервера приложений находится в файле `readme.txt` дистрибутива обновления.

Порядок обновления соответствующего адаптера интеграции находится в файле `changes.txt` дистрибутива адаптера.

В случае возникновения каких-либо вопросов при обновлении свяжитесь со службой внедрения и сопровождения компании «БИФИТ»:

Тел.: (495) 532-15-02, (499) 705-01-01

E-mail: support@bifit.com