Разнесение двух Серверов Приложения iBank 2 UA

Техническое руководство для банковских автоматизаторов (версия 1.0)

Оглавление

Глава 1

Введение

Суть проблемы и назначение документа

Данный документ описывает процедуру разнесения работающего в банке Сервера Приложения iBank 2 UA на два экземпляра. Также будет рассмотрены особенности установки обновления на каждый из этих Серверов Приложения (далее – СП).

Разнесение СП iBank 2 UA на два экземпляра используется для следующих целей:

- Снижение нагрузки на сервер, на котором работает внешний СП;
- Повышение общего уровня надёжности и безопасности системы.

В случае одновременной эксплуатации в банке двух СП iBank 2 UA их роли таковы:

Внешний СП обслуживает корпоративных и частных клиентов банка и доступен по сети Интернет;

Внутренний (внутрибанковский) СП обслуживает операционистов юридических и физических лиц, администраторов банка. К нему подключается серверная часть шлюза, и этот СП доступен только в локальной сети банка. Применение второго СП целесообразно в том случае, если обслуживанием клиентов банка занимается значительное количество банковских сотрудников, работа которых в системе создаёт ощутимую нагрузку на единичный экземпляр СП. В этом случае способом снижения нагрузки на внешний СП и улучшения качества обслуживания клиентов является эксплуатация внутрибанковского СП iBank 2 UA.

Физически оба СП эксплуатируются в локальной сети банка на разных серверах[1] и используют одну БД iBank 2 UA. В данном руководстве предполагается, что в банке *уже установлен* работающий *внешний* СП. На *первом* этапе будет описан процесс построения на его основе внутреннего СП для банковских сотрудников. На *втором* этапе рассмотрим процедуру установки обновления на разнесённые СП с учётом специфики их эксплуатации.

Процедура установки СП iBank 2 UA из дистрибутива описана в документации ***Установка системы iBank 2 UA под Windows (Unix)***.

Наглядно схемы эксплуатации одного и двух СП iBank 2 UA в банке представлены на рисунках ниже.

[1] Возможна эксплуатация нескольких СП на одном сервере с единым IP-адресом.

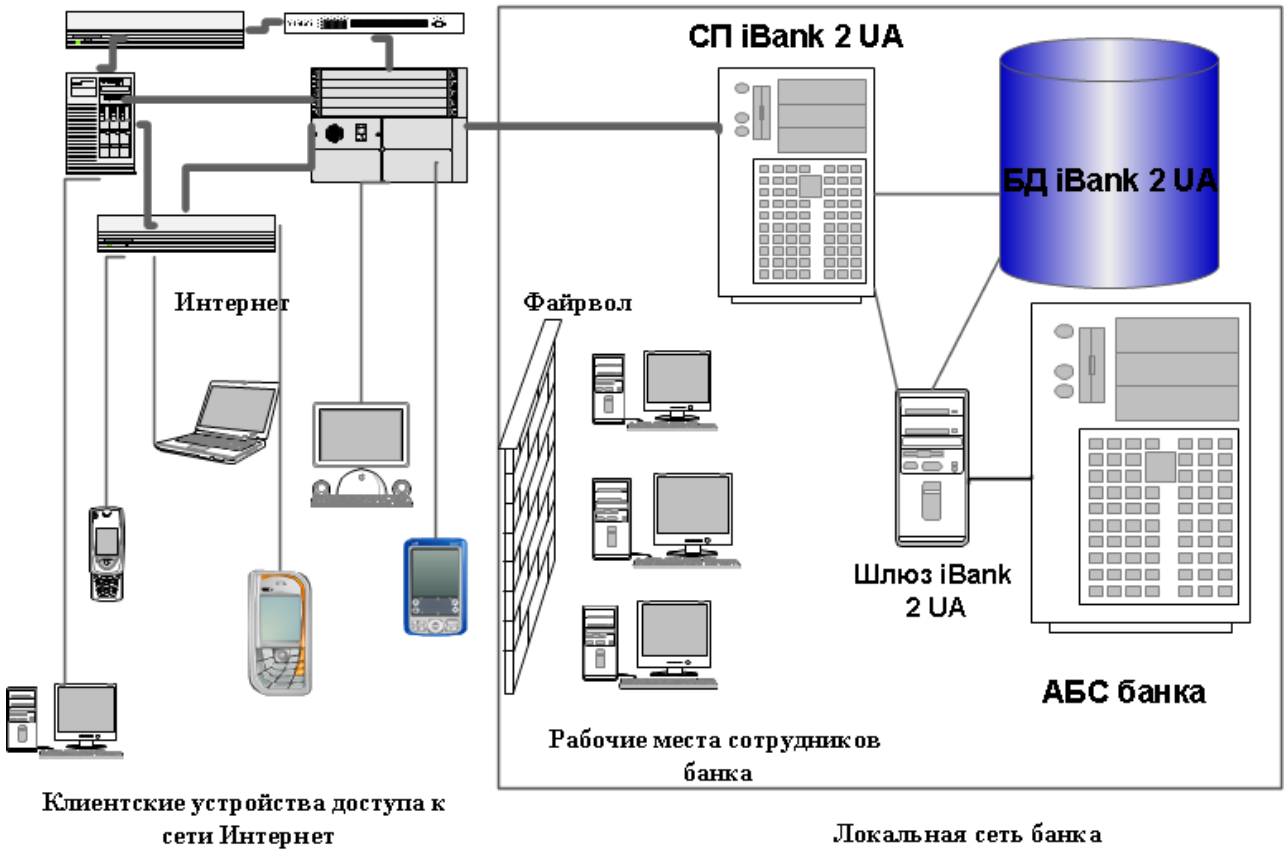


Рис. 1.1. Схема эксплуатации в банке одного СП iBank 2 UA

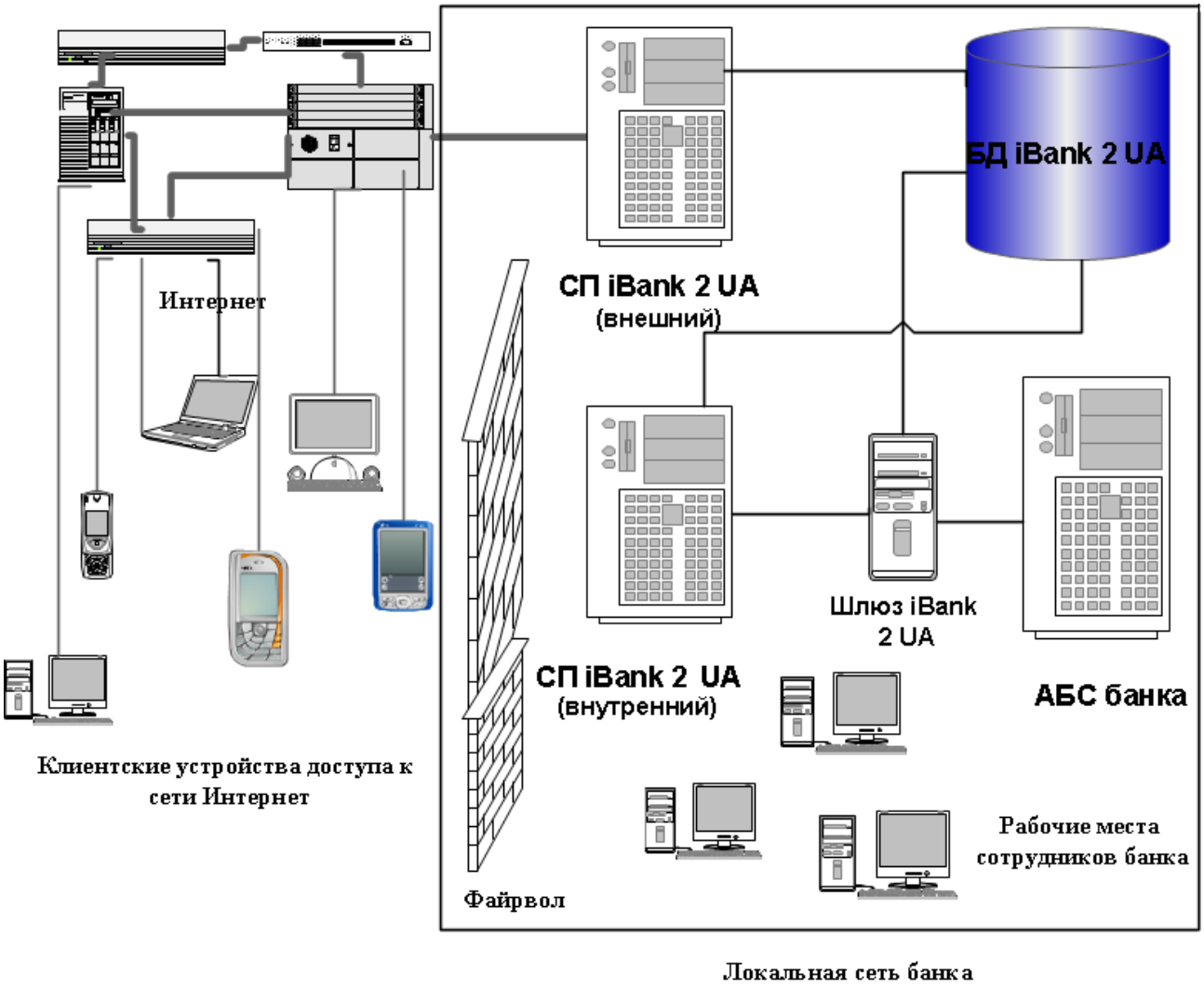


Рис. 1.2. Схема эксплуатации в банке двух СП iBank 2 UA

Глава 2

Разнесение двух Серверов Приложения

Создание внутреннего Сервера Приложения iBank 2 UA

Предварительным этапом к созданию внутреннего (внутрибанковского) СП является выделение сервера, его настройка и подключение к локальной сети банка.
Возможна установка двух СП в следующих вариантах:

- на одном физическом сервере с одним IP-адресом;
- на одном физическом сервере, но на разных виртуальных хостах с разными IP-адресами;
- отдельно на двух физических серверах с разными IP-адресами.

Копирование каталога с внешним Сервером Приложения

Установка внутрибанковского СП начинается с создания копии каталога внешнего СП на внутреннем сервере[1]. В каталоге – копии СП следует проверить и, при необходимости, перенастроить переменные окружения `JAVA_HOME` и `IBANK_HOME` в файле setEnviornment.bat каталога bin. Если виртуальная Java-машина JRE не установлена на новом сервере, то рекомендуется установить её в каталог с СП в папку, к примеру, jre.

Настройка подключения к БД iBank 2 UA

Настройка подключения к БД iBank 2 UA осуществляется в файле connection.xml, который располагается в подкаталоге `conf` в каталоге с СП. Проверьте в этом файле правильность IP-адреса к серверу БД iBank 2 UA.

Настройка разнесённых Серверов Приложения iBank 2 UA

Настройка серверных точек входа и портов разнесённых Серверов Приложения

Следующим этапом настройки разнесённых СП после проверки подключения к БД iBank 2 UA является настройка портов, которые будут слушать эти СП. Настройка серверных точек входа осуществляется в файлах server.xml и остальных xml-файлах с префиксом apps- в папке СП conf. Взаимодействие конечных пользователей с СП происходит по двум протоколам: HTTPS и IBTP. Соответственно, необходимо сконфигурировать порты этих протоколов и доступ к ним на **каждом** из СП.

[1]Здесь и далее, слово «сервер» подразумевается как аппаратно – программная абстракция для обозначения физической или виртуальной машины, на которой будет размещаться и функционировать экземпляр СП.

Конфигурирование протокола HTTPS. По умолчанию, СП слушает этот протокол на 443-м порту. В случае с разнесением СП существуют две ситуации:

1. СП находятся на разных серверах (имеют разный IP-адрес). В этом случае оба СП можно настроить на прослушивание 443-го порта.
2. СП находятся на одном сервере и имеют один IP-адрес. В этом случае для предотвращения конфликта портов на внутрибанковском СП следует поменять порт для прослушивания HTTPS таким образом, чтобы он не совпадал с портом внешнего СП. К примеру, на внутрибанковском сервере можно установить порт для прослушивания 444. Убедитесь, что на назначаемом порту не прослушивается больше никаких сервисов.
3. СП находятся на одном сервере, но для обращения к ним используются разные IP-адреса (технология виртуальных хостов). В этом случае оба СП можно настроить на прослушивание 443-го порта, прописанного по умолчанию.

Конфигурирование протокола IBTP. По умолчанию, СП слушает запросы клиентских апплетов по этому протоколу на порту 9091, апплетов операционистов и администраторов банков – на порту 9092. Как и в случае с протоколом HTTPS, возможны следующие ситуации:

1. Разнесённые СП находятся на разных хостах с разными IP-адресами. При всех раскомментированных точках входа в настройках серверов конфликта портов быть не должно.
2. Разнесённые СП находятся на одном хосте с одинаковым IP-адресом. В этом случае рекомендуется на *внешнем* сервере закомментировать точку входа для операционистов, а на *внутрибанковском* сервере – закомментировать точку входа для клиентов[2].
3. Разнесённые СП находятся на одном сервере, но располагаются на разных виртуальных хостах и имеют разные IP-адреса. Конфликта портов быть не должно при всех раскомментированных точках входа.

При использовании разнесённых СП из соображений безопасности настоятельно рекомендуется закрыть точку входа для банковских сотрудников на внешнем СП.

> ***Внимание:***
> Если в файле server.xml вы настроили порт для протокола IBTP, отличный от 9091 и 9092, поменяйте его в соответствующих файлах конфигурации серверных модулей в папке conf (файлы apps-*.xml).

Конфигурирование порта обработчика AJP. Обработчик AJP предназначен для остановки СП. По умолчанию, этот обработчик слушает порт 8011. Как и в случае с настройкой портов протоколов HTTPS и IBTP, если разнесённые СП находятся на одном сервере, то им необходимо прописать отличающиеся порты для обработчика AJP. К примеру, внутрибанковскому СП можно назначить порт не 8011, а 8012. При этом на назначаемом порту не должно быть никаких посторонних сервисов.

Настройка точек входа клиентских модулей

Конфигурационные файлы с настройками клиентских точек входа на СП находятся в каталоге СП webapps\ROOT и представляют собой xml – файлы. Настройке подлежат следующие файлы на ***обоих*** СП: `administrator.xml`, `client.xml`, `multiclient.xml`, `operator.xml`, `poperator.xml`, `makekeys.xml`, `pclient.xml`. В этих файлах необходимо указать или, при необходимости, закомментировать, точки входа для клиентов банка или банковских сотрудников, в зависимости от конкретного экземпляра СП и, соответственно, настроек файла server.xml. Например, если на внешнем сервере принято решение закрыть точки входа для операционистов и администраторов банка, то необходимо закомментировать точки доступа в следующих файлах: `administrator.xml`, `operator.xml` и `poperator.xml`. На внутрибанковском

[2] В этом случае, если на внутрибанковском сервере не будут закрыты точки входа для клиентских модулей, банковские сотрудники смогут использовать ресурсы двух СП одновременно. Подробнее об этом читайте в подразделе **Одновременное использование банковскими сотрудниками разнесённых Серверов Приложения**.

сервере точки входа в файлы с клиентскими настройками не рекомендуется комментировать, так как в этом случае банковские сотрудники не смогут войти через внутрибанковский сервер, к примеру, под тестовым клиентом - юридическим лицом и будут вынуждены использовать для этих целей внешний или иной СП.
Файлы, которые содержат ненужные точки доступа, можно вообще удалить. Этот вариант более предпочтителен, если никаких перенастроек точек входа в дальнейшем не планируется.
Об особенностях настройки файла makekeys.xml на внутрибанковском СП читайте в подразделе **Особенности использования АРМа Регистратор банковскими сотрудниками**.

Тестирование настроек разнесённых Серверов Приложения

После настройки подключения к БД iBank 2 UA, настройки портов обоих СП можно проверить работоспособность связки **Внешний СП** $\Longleftrightarrow$ **БД iBank 2 UA** $\Longleftrightarrow$ **Внутренний СП**.

В первую очередь необходимо осуществить запуск *внутреннего* СП. Стабильная работа этого экземпляра СП будет свидетельствовать о целостности его каталогов и правильности настроек для подключения к БД. Убедившись в корректности работы внутреннего СП, запустите *внешний* СП. На этом этапе проверяется корректность настройки портов обоих СП. Если какие-то протоколы (HTTPS, IBTP, обработчик AJP) конфликтуют между собой из-за совпадения портов, то это вызовет аварийную остановку *обоих* экземпляров СП. При этом следует учесть, что даже при наличии конфликта портов СП их аварийная остановка происходит *не сразу*. Об отсутствии конфликта портов свидетельствует нормальная работа обоих СП в течение минимум минуты.

Глава 3

Эксплуатация разнесённых Серверов Приложения iBank 2 UA

Особенности входа на внутрибанковский Сервер Приложения

Для клиентов банка наличие двух разнесённых СП прозрачно и не требует использования настроек или адресов, отличных от тех, что применялись до разнесения СП.
Иначе обстоит ситуация с входом на *внутрибанковский* СП. Если внутрибанковский СП работает на отдельном хосте и использует стандартный HTTPS – порта, то для входа на главную страницу внутрибанковского сервера необходимо указать в строке браузера следующее:
https://<www илиIP-адрес>/index_bank.html.

Если же внутрибанковский СП работает на том же сервере, что и внешний, и/или на нём используется нестандартный порт для протокола HTTPS[1], то в строке браузера банковским сотрудникам необходимо будет указывать следующее: ***https://<www или IP-адрес>:<номер порта>/index_bank.html***. К примеру, если внутрибанковский СП развёрнут на хосте с IP-адресом 192.168.10.123 и портом HTTPS 444, строка для браузера будет следующей: `https://192.168.10.123:444/index_bank.html`.

Особенности использования АРМа Регистратор банковскими сотрудниками

В случае, если на внутрибанковском СП *не предусмотрено* использование серверной точки входа для клиентских модулей (соответствующая секция закомментирована в файле server.xml), то для регистрации новых банковских сотрудников без специальных настроек придётся полностью использовать ресурс внешнего СП[2].

Перенастроив АРМ **Регистратор**, можно частично или полностью перенести нагрузку, связанную с его использованием, с внешнего на внутрибанковский СП. Существуют два варианта настроек:

Частичное использование обоих СП. В этом случае в файле makekeys.xml в каталоге СП webapps\ROOT необходимо указать в секции <transport> адрес *внешнего* СП, в то же время в секции <makekeys> следует указать адрес *внутрибанковского* СП. Для запуска апплета **Регистратор** банковские сотрудники будут использовать адрес и, соответственно, веб-сервер внутрибанковского СП, а взаимодействие апплета будет происходить с внешним СП.

Полная разгрузка внешнего СП. Данный вариант представляется наиболее оптимальным. Для реализации этой возможности следует перенастроить стандартный порт АРМа **Регистратор** на порт, который используют апплеты АРМов **Операционист** и **Администратор банка**[3]. В файле

[1] Стандартный порт протокола HTTPS — 443.
[2] АРМ **Регистратор** банковских сотрудников использует клиентский порт входа 9091.
[3] Стандартный порт для этих АРМов – 9092.

apps-registry.xml в каталоге conf внутрибанковского СП и в файле makekeys.xml в каталоге внутрибанковского СП webapps\ROOT следует указать открытый для остальных банковских АРМов порт. В этом случае для запуска апплета **Регистратор** банковские сотрудники будут использовать как веб-сервер, так и собственно сам СП, установленный специально для них.

Одновременное использование банковскими сотрудниками разнесённых Серверов Приложения

В том случае, если на внутрибанковском СП закрыта точка входа только на стороне сервера, в то время как клиентские точки входа открыты, внутрибанковский СП можно использовать как веб-сервер. Загруженные апплеты, при наличии необходимых настроек, смогут работать с другим экземпляром СП. Для этого необходимо в настройках требуемых апплетов указать в секции <transport> адрес другого СП. Подробнее о том, как это сделать на примере АРМа **Регистратор**, читайте в подразделе **Особенности использования АРМа Регистратор банковскими сотрудниками**.

Данная схема работы может быть применена в крупных банках, где ресурсов серверов с двумя СП недостаточно для комфортной работы пользователей. В этом случае можно настроить и эксплуатировать в банке несколько разнесённых СП. Их роли можно распределить следующим образом (если используются 3 СП):

- Внешний СП занимается исключительно обслуживанием клиентов банка;
- СП для банковских сотрудников служит частично или полностью веб-сервером для входа в АРМы банковских сотрудников;
- Вспомогательный СП обрабатывает запросы АРМов банковских сотрудников и работает с Шлюзом iBank 2 UA.

Особенности настройки Шлюза

При разнесении Сервера Приложения на два экземпляра Шлюз-сервер устанавливается в головном банке и работает в рамках Внутреннего Сервера Приложения, а Шлюзы-клиенты устанавливаются в филиалах. Если разнесенные СП находятся на одном хосте с одинаковым IP-адресом и для Внутреннего СП был изменён порт 9091, то на всех Шлюзах-клиентах необходимо изменить настройки подключения на новый порт.

Для того, чтобы не использовался старый Шлюз-сервер необходимо произвести шаги обратные установке и удалить ранее сгенерированные ключи Шлюз-сервера.

Общие замечания по безопасности

Использование двух разнесённых СП повышает общий уровень безопасности в банке, полностью интегрируя внутрибанковский СП в локальную сеть банка. Тем не менее, для безопасной эксплуатации разнесённых СП следует придерживаться следующих рекомендаций:

- *На внешнем СП.* Закрыть файрволом неиспользуемые порты для протокола IBTP и порт обработчика AJP, закрыть точку входа для банковских сотрудников в настройках сервера (server.xml) и в настройках клиентских модулей (в каталоге webapps\ROOT). Как минимум, следует закрыть серверную точку входа.
- *На внутрибанковском СП.* При необходимости, можно закрыть на этом СП все серверные и клиентские точки входа для клиентских апплетов. В этом случае банковские сотрудники для входа в клиентские АРМы будут полностью или частично использовать внешний СП.
- При *частичном использовании* банковскими сотрудниками двух СП для АРМа **Регистратор**[4] (см. подраздел **Особенности использования АРМа Регистратор банковскими сотрудниками**)

[4]Или других, недоступных на данном сервере АРМов.

в секции <transport> в файле makekeys.xml рекомендуется указать внутренний IP-адрес внешнего сервера.

- Использование в секции <transport> в xml – файлах в каталоге webapps\ROOT IP-адреса 127.0.0.1 сделает невозможным загрузку апплетов с удалённых компьютеров по локальной сети. К примеру, если в банке только один сотрудник зарегистрирован как Администратор банка в системе iBank 2 UA, то для повышения безопасности можно настроить доступ и, соответственно, возможность работы с этим АРМом только на той машине, на которой работает внутрибанковский СП.

Глава 4

Установка пакета обновлений на разнесённые Сервера Приложения iBank 2 UA

В данной главе содержится описание процедуры установки обновления на разнесённые СП iBank 2 UA с использованием стандартных пакетов обновлений iBank 2 UA. Особенностью установки обновления при эксплуатации разнесённых СП является необходимость перенастройки конфигурационного файла пакета обновлений при установке на внутрибанковский СП с учётом использования совместной БД iBank 2 UA. Исходя из этого, основные стадии установки обновления на оба СП таковы:

- Стандартная установка обновления для внешнего СП и БД;
- Перенастройка конфигурационного файла пакета обновления;
- Установка обновления для внутрибанковского СП.

Подробно эти стадии будут описаны ниже.

Подготовительный этап

На подготовительном этапе следует выполнить следующие действия:

- Остановить оба разнесённых СП;
- Подготовить копии каталогов разнесённых СП;
- Сделать резервную копию БД iBank 2 UA.

Особое внимание следует уделить наличию резервных копий файлов из каталога conf и webapps\ROOT для каждого из СП.

Установка обновления на внешний Сервер Приложения

Подробно *стандартная* процедура установки обновления описана в инструкции к пакету обновлений. В данном руководстве вкратце рассмотрим эти этапы:

- Автоматическое обновление БД iBank 2 UA;
- Автоматическое обновление библиотек и других файлов собственно СП;
- Ручное обновление файлов каталога webapps\ROOT.

При замене файлов каталога webapps\ROOT следует убедиться, что оригинальные файлы конфигурации разнесённого СП (xml-файлы) не затёрты стандартными файлами из пакета обновления. В случае если часть этих оригинальных файлов всё же требуется заменить, проставьте в них настройки портов и адресов из резервной копии данного разнесённого СП.

Перенастройка конфигурационного файла пакета обновления

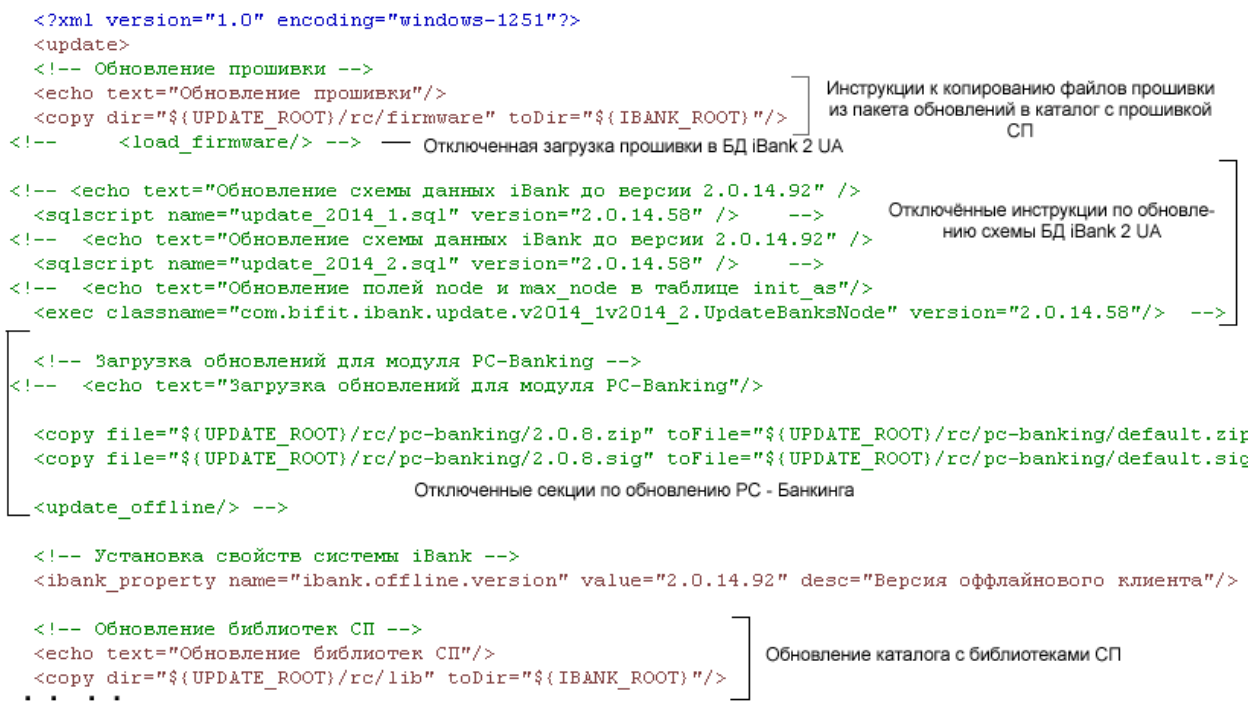
В стандартном пакете обновления iBank 2 UA настраиваются два файла[1]:

- `UPDATE_ROOT\bin\update.bat`. В этом файле настраивается путь к корневому каталогу разнесённого СП. Перед установкой обновления убедитесь, что в нём указан путь к требуемому СП.
- `UPDATE_ROOT\update.xml`. В этом файле содержатся инструкции, что, как и откуда следует обновлять в каталогах СП и БД. Для корректной установки обновления на внутрибанковский СП необходимо отключить (закомментировать) в файле update.xml следующие секции настроек:

  1. инструкции к обновлению БД iBank 2 UA (обязательно);
  2. загрузку прошивки в БД iBank 2 UA (повторная загрузка только отнимает время);
  3. обновление РС – Банкинга (не используется банковскими сотрудниками).

  Если в файле update.xml отсутствуют инструкции к обновлению БД, то этот пункт пропускается.

  На рис. 4.1 рассмотрен пример содержания файла update.xml из пакета обновлений для стандартной версии iBank 2 UA 2.0.14.92 с комментариями к секциям.




```
<?xml version="1.0" encoding="windows-1251"?>
<update>
<!-- Обновление прошивки -->
<echo text="Обновление прошивки"/>
<copy dir="${UPDATE_ROOT}/rc/firmware" toDir="${IBANK_ROOT}"/>
<!--     <load_firmware/> -->

<!-- <echo text="Обновление схемы данных iBank до версии 2.0.14.92" />
  <sqlscript name="update_2014_1.sql" version="2.0.14.58" />    -->
<!--  <echo text="Обновление схемы данных iBank до версии 2.0.14.92" />
  <sqlscript name="update_2014_2.sql" version="2.0.14.58" />    -->
<!--  <echo text="Обновление полей node и max_node в таблице init_as"/>
  <exec classname="com.bifit.ibank.update.v2014_1v2014_2.UpdateBanksNode" version="2.0.14.58"/>  -->

  <!-- Загрузка обновлений для модуля PC-Banking -->
<!--  <echo text="Загрузка обновлений для модуля PC-Banking"/>

  <copy file="${UPDATE_ROOT}/rc/pc-banking/2.0.8.zip" toFile="${UPDATE_ROOT}/rc/pc-banking/default.zip
  <copy file="${UPDATE_ROOT}/rc/pc-banking/2.0.8.sig" toFile="${UPDATE_ROOT}/rc/pc-banking/default.sig
  <update_offline/> -->

  <!-- Установка свойств системы iBank -->
  <ibank_property name="ibank.offline.version" value="2.0.14.92" desc="Версия оффлайнового клиента"/>

  <!-- Обновление библиотек СП -->
  <echo text="Обновление библиотек СП"/>
  <copy dir="${UPDATE_ROOT}/rc/lib" toDir="${IBANK_ROOT}"/>
  . . . .
```

Рис. 4.1. Фрагмент файла update.xml

Установка обновления для внутреннего Сервера Приложения

Окончательно проверив правильность настроек конфигурационного файла пакета обновлений, можно приступать к установке обновления для файлов внутрибанковского СП. Следует отметить, что если БД iBank 2 UA *уже была обновлена*, то при повторной попытке изменить БД процедура обновления завершится с ошибкой, и некоторые файлы СП *не будут обновлены*. В этом случае необходимо восстановить СП из резервной копии, проверить настройки файла update.xml и повторить процедуру установки обновления.

[1] UPDATE_ROOT – условное обозначение корневого каталога с разархивированным обновлением.

После автоматической замены файлов СП и ручного копирования новых версий файлов в каталог webapps\ROOT убедитесь, что сохранены настройки портов и хостов данного разнесённого СП (см. подраздел **Установка обновления на внешний Сервер Приложения**).

После успешной установки обновления на все СП и БД необходимо проверить их работоспособность. Для этого запустите разнесённые СП, проверьте возможность входа под тестовыми пользователями в клиентские и банковские АРМы; их корректное функционирование. При обнаружении ошибок в работе разнесённых СП обратитесь в службу технической поддержки компании «БИФИТ».

Глава 5

Источники дополнительной информации

С дополнительной информацией по данной тематике можно ознакомиться в документах:

- ***Общая информация о системе iBank 2 UA***
- ***Выбор аппаратного и программного обеспечения для работы системы iBank 2 UA***
- ***Механизмы безопасности в системе iBank 2 UA***
- ***Установка системы iBank 2 UA под ОС Windows/Unix***
- ***Файловая структура Сервера Приложения iBank 2 UA***

Примечание:
Со всеми предложениями и пожеланиями по документации обращайтесь по электронному адресу support@bifit.com.ua