БФТ ЭКСПЕРТ

«Документооборот «ДоксЛоджик» (DoXLogic)»

Руководство по установке

2016 г.

Аннотация

Данный документ содержит инструкции по инсталляции системы документационного обеспечения управления (в дальнейшем – Система).

В документе приведено описание процесса установки клиентских компонент для Desktop-версии Системы и инструкции по инсталляции WEB-модуля Системы, обеспечивающего возможность удаленной работы пользователей с помощью стандартного браузера MS Internet Explorer.

В документе приведено описание процесса установки серверных и клиентских компонент. Руководство ориентировано на сотрудников информационно-технических подразделений.

Документ соответствует версии программного продукта DoXLogic v.3.5.3.

Оглавление

1. Общий порядок действий при установке Системы

Для установки всех компонент Системы необходимо последовательно выполнить следующие действия:

- Подготовить конфигурацию серверной группы, соответствующей требованиям, изложенным в документе «Требования к аппаратно-программной части для эксплуатации СЭД DoXLogic».
- Установить серверную часть Системы (базу данных).
- Установить и настроить сервер приложений Системы, включая:
  - JAVA машину;
  - WEB-сервер;
  - Приложение Системы;
  - Прикладные модули Системы.
- Выполнить настройку службы управления паролями доступа.
- Установить клиентскую часть Системы на рабочие места пользователей.

Компоненты системы содержатся в дистрибутиве, который имеет следующую структуру каталогов:

Properties – файлы конфигурации.

Web – компоненты, относящиеся к установке сервера приложений.

В дистрибутив включены следующие файлы:

В корневом каталоге:

- DATABASE_DRBxxxx_DFAxxxx_MSSQL2008.rar – заархивированный образ БД для MSSQL 2008 и выше (где xxxx – номера версий).
- Documentation.rar – архив документации.
- jAllDesktop.rar – заархивированный Desktop-Клиент Системы.
- DoXLogicServices_Setup.exe – инсталлятор Служб Системы.
- PDFiFilter64installer.zip – инсталлятор фильтра для настройки полнотекстового поиска по содержимому pdf-файлов (64 бит).
- FilterPackx64.exe - инсталлятор фильтра для настройки полнотекстового поиска по содержимому файлов пакета Office2007 (64 бит).

В каталоге Scripts:

- SET Zirvan.txt – текстовый файл с командой для создания пользователя Zirvan в БД и включении полнотекстового поиска

Каталог properties:

- properties_mssql_desktop – конфигурационный файл для Desktop-Клиента Системы (MSSQL).
- properties_oracle_desktop – конфигурационный файл для Desktop-Клиента Системы (ORACLE).
- properties_oracle_scheduler – конфигурационный файл для Службы jScheduler (MSSQL).
- properties_mssql_scheduler – конфигурационный файл для Службы jScheduler (ORACLE).
- properties_mssql_web – конфигурационный файл для WEB-Сервера (MSSQL).
- properties_oracle_web – конфигурационный файл для WEB-Сервера (ORACLE).
- jcifs.properties – конфигурационный файл NTLM для WEB-Сервера.

- log4j.properties – конфигурационный файл логгера для WEB-Сервера.

Каталог Web:

- apache-tomcat-7.0.68.exe – инсталлятор Томкат Web-Сервера.
- jdk-7u85-windows-i586.exe – инсталлятор 32-бит JAVA-Машины.
- jdk-7u85-windows-x64.exe – инсталлятор 64-бит JAVA-Машины.
- Docflow.war – WEB-приложение.
- Delete_Classes.cmd – исполняемый файл для очистки кэша WEB-приложения.
- CAPICOM2102.rar – архив с инсталлятором библиотеки CAPICOM, предоставляющей COM-интерфейс, использующий основные функции CryptoAPI.
- ZirvanrootCA.zip – сертификат, необходимый для обеспечения работоспособности java-апплетов системы.

2. Установка серверной части Системы (базы данных)

Установка серверной части Системы должна выполняться на компьютере, выделенном под сервер базы данных. Выполнять установку должен администратор СУБД, с использованием файлов **DATABASE_DRBxxxx_DFAxxxx_MSSQL2008.rar** и **SET Zirvan.txt** дистрибутива.

Для инсталляции Системы на сервер базы данных администратор СУБД MSSQL должен выполнить следующие действия:

1. Создать учетную запись **zirvan** в СУБД MSSQL 2008.
2. Развернуть средствами Server Management Studio СУБД MSSQL 2008 (далее БД) начальный дамп Системы – файл **DATABASE_DRBxxxx_DFAxxxx_MSSQL2008.dmp** из архива **DATABASE_DRBxxxx_DFAxxxx_MSSQL2008.rar**. При этом желательно разнести файлы БД по разным физическим дискам.
3. Подсоединиться к БД от имени администратора и выполнить следующие команды **sp_change_users_login 'Auto_Fix', 'zirvan', NULL** и **sp_fulltext_database 'enable'**
4. Настроить Maintenance Plan для созданной БД по следующей схеме:
   - Полный backup БД раз в неделю (ночь в выходные)
   - Backup транзакционных логов – каждый час в рабочее время
   - Сбор статистики по БД (sample – 10-25%) – раз в месяц (первый месяц работы желательно каждый день).

3. Установка 32-бит версии сервера приложений Системы

Установка сервера приложений Системы должна выполняться на компьютере, выделенном под сервер приложений. Выполнять установку должен администратор Системы, с использованием файлов из каталога **Web** дистрибутива.

3.1. Установка JAVA-машины

Для работы сервера приложений Системы необходимо установить 32-бит версию JDK (J2SE Development Kit) версии 7. Ниже приведен порядок его установки:

1. Запустить инсталлятор **WEB\jdk-7u85-windows-i586.exe** из дистрибутива Системы, который последовательно установит следующее программное обеспечение:
   - Java SE Development Kit 7;
   - Java Runtime Environment 7.
2. Во время инсталляции «Java SE Development Kit 7» необходимо изменить каталог установки «Development Tools» с предлагаемого по умолчанию адреса на **C:\Java\jdk7**, как показано на Рис. 1.

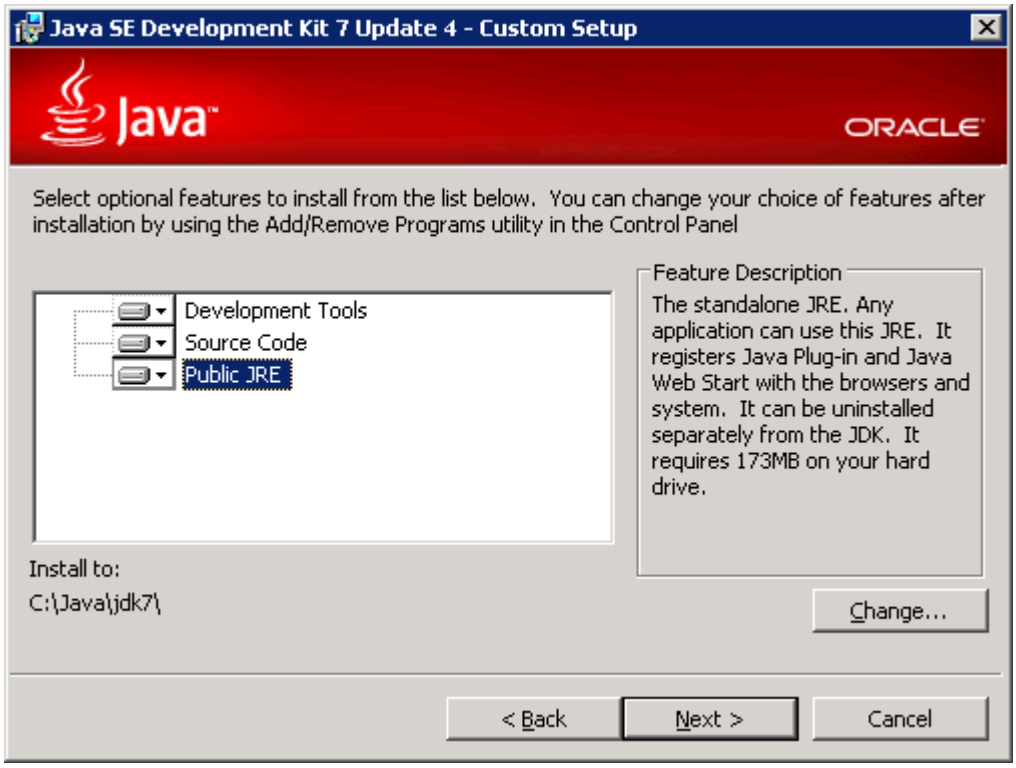


Рис. 1. Установка Java SE Development Kit 7

3. После нажатия на кнопку «Next» инсталлятор установит «Java SE Development Kit 7», после чего автоматически запуститься установка «Java Runtime Environment 7».

Во время инсталляции «Java Runtime Environment 7» необходимо изменить каталог установки предлагаемого по умолчанию адреса на C:\Java\jre7\, **а состав устанавливаемых компонент оставить таким, какой предлагается по умолчанию, см. Рис. 2. Установка Java Runtime Environment 7**

4. По завершении процесса инсталляции на экране отобразится сообщение «**Installation Completed**» и будет запущен процесс регистрации, который можно пропустить.
5. .

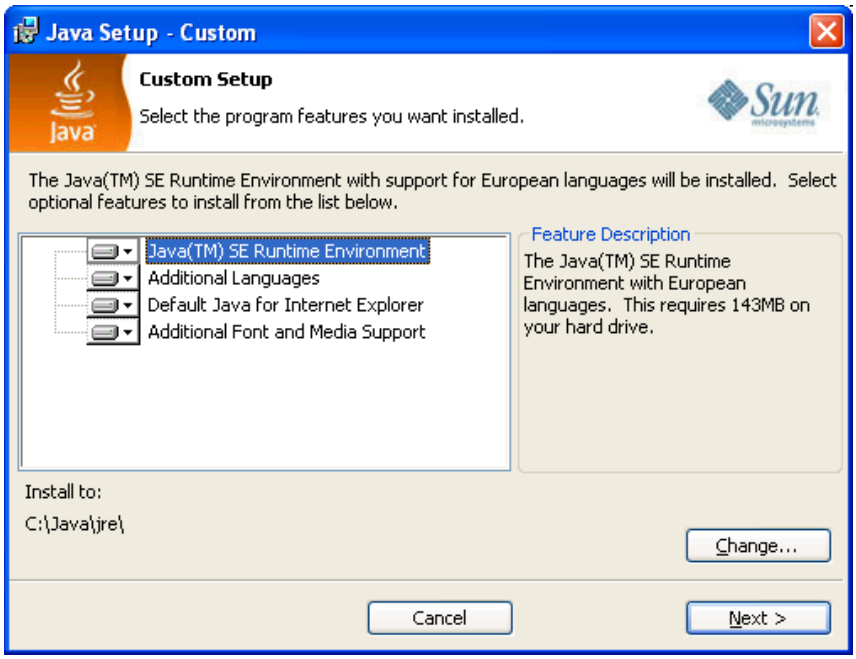


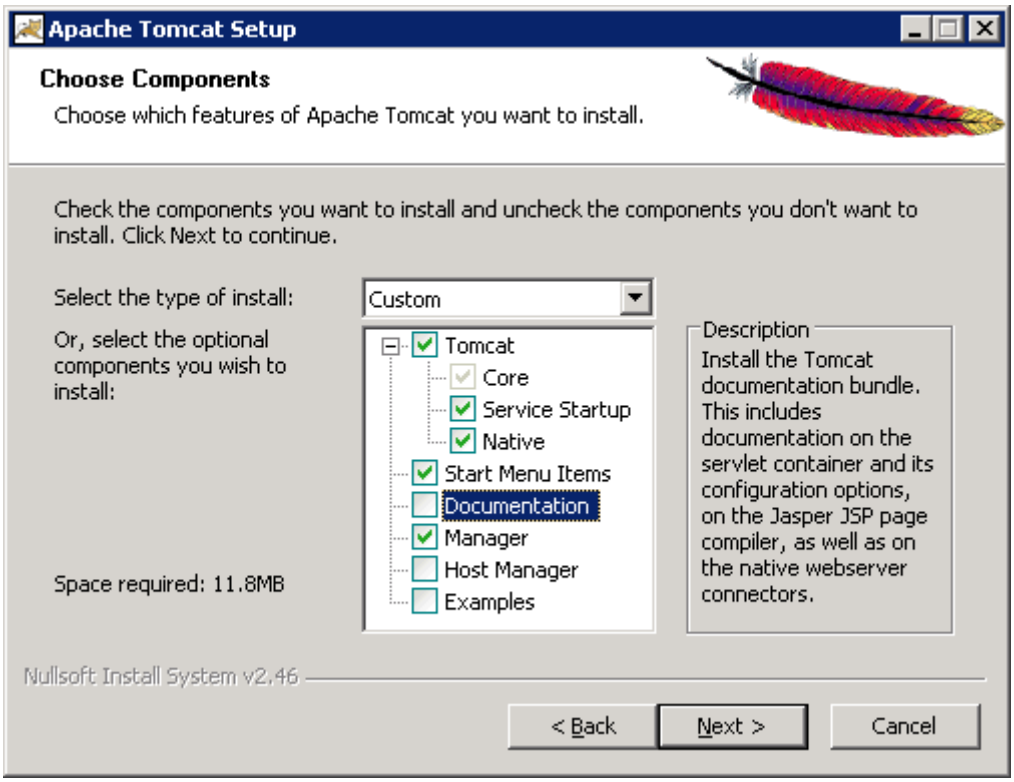
Рис. 2. Установка Java Runtime Environment 7

6. По завершении процесса инсталляции на экране отобразится сообщение «**Installation Completed**» и будет запущен процесс регистрации, который можно пропустить.

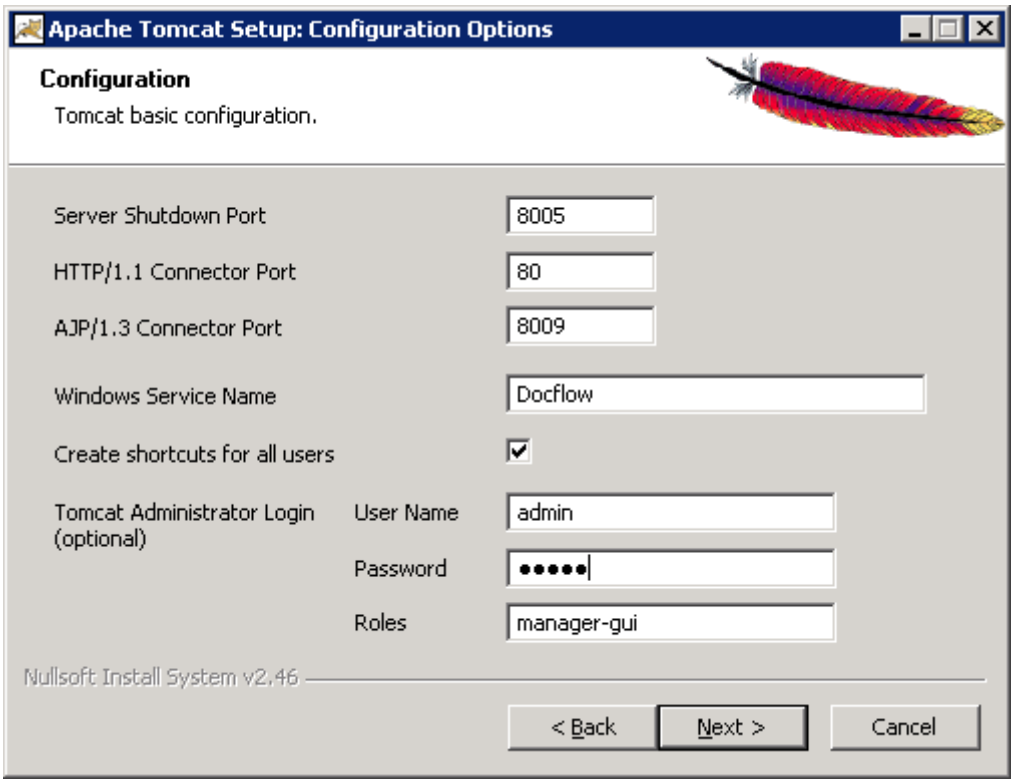
3.2. Установка сервера приложений «Application Server Tomcat»

Для 32 битной ОС:

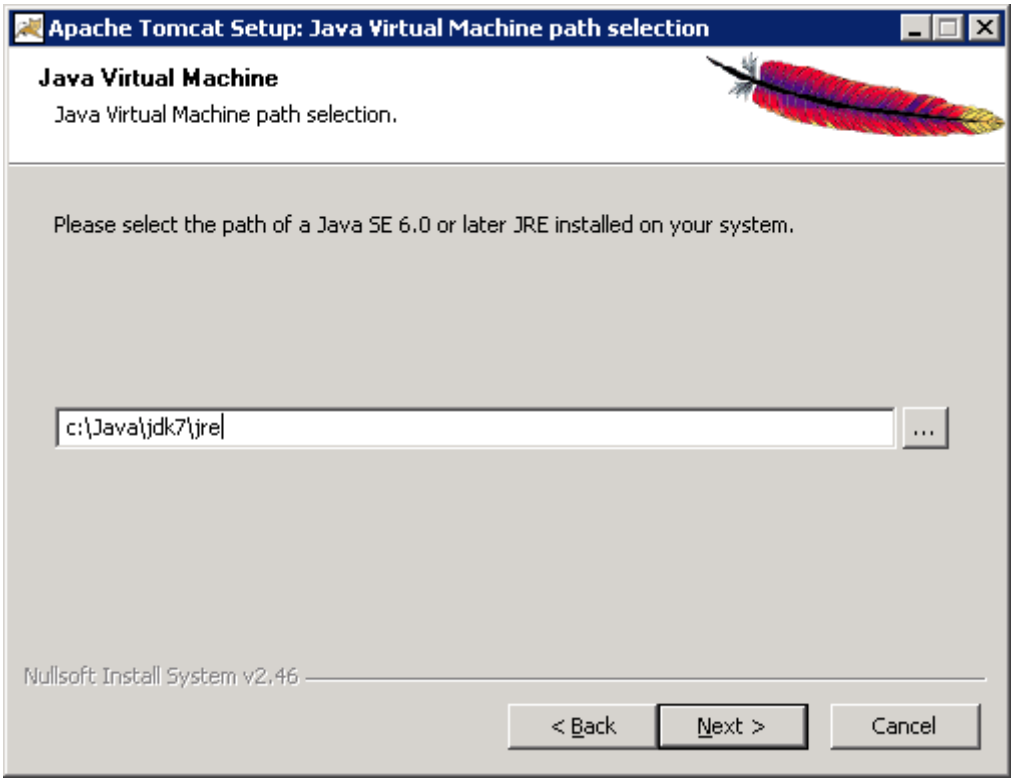
1. Запустить инсталлятор из Дистрибутива **Web/apache-tomcat-7.0.68.exe**
2. Выбрать необходимые компоненты, как на рисунке



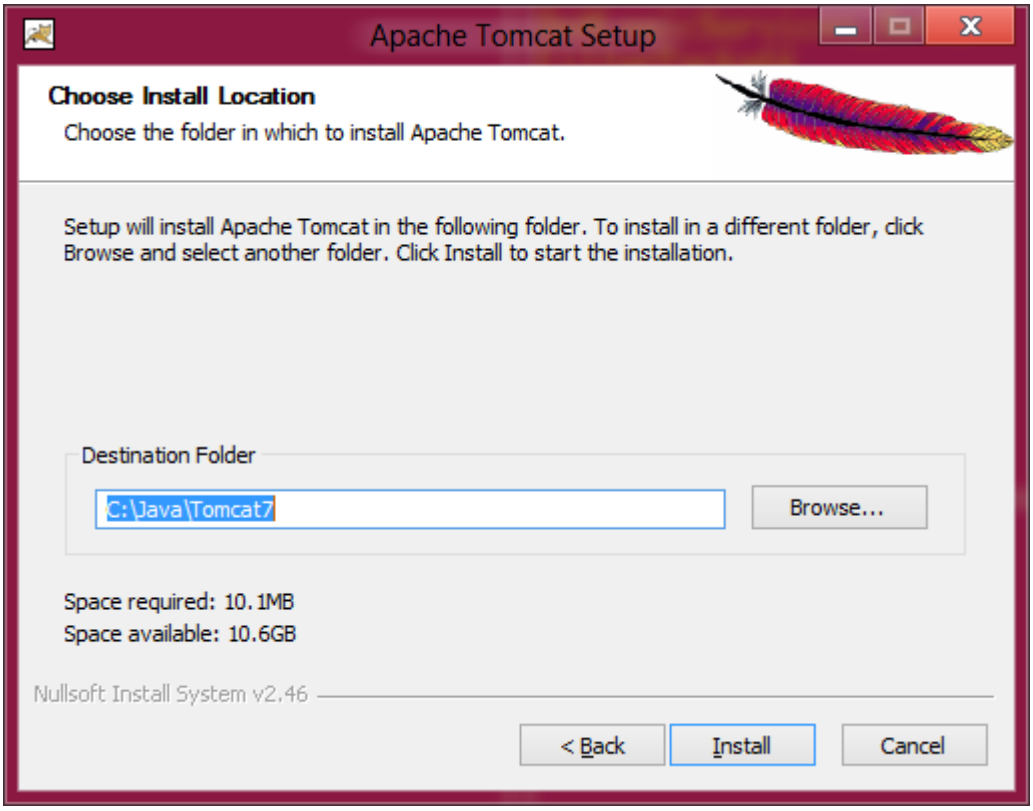
3. Указать порт, название службы и реквизиты администратора для Tomcat’а



4. И указать путь к установленной JAVA Virtual Machine:



5. Инсталляцию надо произвести в каталог **c:\Java\Tomcat7**:



Для 64 битной ОС:

Убедиться в наличии файлов **msvcr100.dll** в каталоге **c:\Windows\System32**, если его нет, то скопировать его в указанный каталог из дистрибутива **Application Server\msvcr100.dll** (а в случае, когда инсталляцию производится на 64-битную версию Windows, то и в каталог **c:\Windows\SysWOW64**).

1. Разархивировать файл с 32-битной версией сервера приложений **apache-tomcat-7.0.68-windows-x86.zip** в каталог **c:\Java\Tomcat7**.
2. Зарегистрировать Windows сервис, выполнив последовательность действий:
    a. Запустить **cmd.exe**;
    b. Перейти в каталог Tomcat, выполнив команду: **cd c:\Java\Tomcat7\bin;**
    c. Запустить командный файл инсталляции службы, выполнив команду: **service.bat install Docflow;**
    d. Убедиться, что в списке служб Windows появилась соответствующая служба. Установить у нее тип запуска в автоматический.
3. Создать ярлык для запуска менеджера сервиса tomcat:
    a. Создать новый ярлык на Рабочем столе, выбрав пункт **New - > Shortcut** из системного меню, вызываемого по нажатию правой кнопкой мыши на Рабочем столе;
    b. В появившемся окне набрать **C:\Java\Tomcat7\bin7\tomcat7w.exe //ES//Docflow** и нажать кнопку <Next>;
    c. Указать наименование для нового ярлыка **- Manage Docflow tomcat -** и нажать кнопку <Finish>.

После установки Tomcat'а следует выполнить следующие операции:

1. Для обеспечения стабильной работы сервиса с большим количеством пользователей необходимо увеличить количество выделяемой сервису оперативной памяти. Для этого необходимо запустить окно настройки сервиса, выполнив последовательность действий:
    a. Запустить созданный ярлык и выбрать закладку «Java»**;**

b. Убедиться, что поле «Java Virtual Machine» указывает на **c:\Java\jdk7\jre\bin\server\jvm.dll;**

c. В поле «Maximum memory pool» указать **1200**;

В поле «Java Options» добавить строки, с обязательным сохранением дефисов: (см. Рис. 3. Выбор количества оперативной памяти

2. В целях безопасности, необходимо отключить возможность удаленного управления, путем блокирования доступа к управляющим приложениям Tomcat с IP адресов отличных от localhost. Для этого в файле ***C:\Java\Tomcat7\webapps\manager\META-INF\context.xml*** тег Context заменяют на:

```
<Context antiResourceLocking="false" privileged="true">
        <Valve className="org.apache.catalina.valves.RemoteAddrValve"
               allow="127.0.0.1"/>
</Context>
```

3. На WEB сервере рекомендуется установить режим динамического сжатия данных, для чего следует скорректировать файл ***C:\Java\Tomcat7\conf****server.xml*, добавив в раздел нужного Connector'а следующие параметры:

```
compressionMinSize="2048"
noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/javascript,text/css"
```

Пример (для типового случая, когда используется только стандартный Connector для порта 80):

```
<Connector port="80" protocol="HTTP/1.1" executor="tomcatThreadPool"
           connectionTimeout="20000"
           redirectPort="443"
           maxThreads="200"
           enableLookups="false" disableUploadTimeout="true"
           acceptCount="200"
           compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml"
           />
```

3.3. Установка прикладных модулей ядра Системы

В состав прикладных модулей ядра Системы, необходимых для работы, входят следующие модули:

- Модуль **jNotifier.Server**, предназначенный для доставки информационных сообщений получателю.
- Модуль **jScheduler.Server**, предназначенный для автоматического выполнения по расписанию пользовательских и служебных заданий.

Для установки этих модулей на сервере приложений необходимо запустить программу инсталлятора **DoXLogicServices_Setup.exe** из дистрибутива и следовать появляющимся на экране инструкциям.

1. По окончании процесса инсталляции появляется сообщение об успешном завершении.
2. Заменить конфигурационный файл **C:\Program Files\CSBI-Zirvan\DoXLogicServices\jScheduler.Server\properties** файлом из Дистрибутива **properties\properties_mssql_scheduler.** В новом файле **properties** отредактировать название Сервера БД и наименование БД:

```
bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://SERVER\:3436;databasename\=DATABASE\:tds\=8.0;l
astupdatecount\=true
```

3. Войти в управление службами ОС Windows, установить сервисы jNotifier.Server и jScheduler.Server в режим автоматического запуска и запустить их на выполнение.
4. Проверить корректность работы сервиса **jNotifier.Server**, для чего убедиться в наличии строки **«Notifier Service started»** в автоматически созданном файле протокола **not_out.txt** (см. каталог установки сервисов).

5. Проверить корректность работы сервиса **jScheduler.Server**, для чего убедиться в отсутствии строк **«error exception»** в автоматически созданном файле протокола **sched_out.txt** (см. каталог установки сервисов).

3.4. Установка приложения Системы на WEB - сервер

Публикация приложения Системы на компьютере сервера приложений осуществляется стандартным для Apache Tomcat способом. Ниже приводится описание порядка установки и начальной настройки приложения.

1. Остановить сервис Apache Tomcat DF с помощью менеджера служб Windows, если он был запущен.
2. Скопировать конфигурационный файл протоколирования **log4j.properties** из каталога properties инсталлятора в каталог ***C:\Java\Tomcat7\conf.***
3. Поместить файл **Web\Docflow.war** из дистрибутива Системы в каталог **C:\Java\Tomcat7\webapps.**
4. Для использования NTLM авторизации следует поместить файл jcifs.properties из дистрибутива в папку **C:\Java\Tomcat7\conf**. В нем нужно указать имя домена (заменив текст DOMAIN в приведенном ниже примере файла), на котором аутентифицируются пользователи Системы, и имя или IP адрес контроллера этого домена (заменив текст DOMAINCONTROLLER в приведенном ниже примере файла). Если контроллер домена требует обязательной предварительной аутентификации, то необходимо указать реквизиты пользователя имеющего права на доступ к Active Directory в поля USERNAME и PASSWORD.

```
jcifs.smb.lmCompatibility=0
jcifs.smb.client.useExtendedSecurity=false
# used when loadBalance=true
jcifs.smb.client.domain=DOMAIN
jcifs.util.loglevel=3
# if empty, will set loadBalance to true
jcifs.http.domainController=DOMAINONTROLLER
#jcifs.netbios.wins=WINSERVERIP1,WINSERVERIP1
jcifs.http.loadBalance=true
jcifs.smb.client.username=USERNAME
jcifs.smb.client.password=PASSWORD
jcifs.smb.client.soTimeout=400000
#jcifs.http.skipAuthList=127.0.0.1
```

   Убедиться, что в политике безопасности домена разрешена NTLMv1 авторизация.

5. Для использования Kerberos авторизации (NTLMv2) необходимо:

   - Отключить NTLM фильтр, если он был включен. Для этого требуется удалить файл C:\Java\Tomcat7\conf\jcifs.properties.
   - После каждой установки обновления web-приложения системы ЭДО необходимо корректировать файл C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml. В нем необходимо раскомментировать тег «filter-mapping» для SPNEGO:

```
<filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
        <url-pattern>/security/*</url-pattern>
</filter-mapping>
```

   - Скопировать из дистрибутива файлы krb5.conf и login.conf в каталог c:\Java\Tomcat7\conf, после чего в файле krb5.conf заменить все слова DOMAIN на NETBIOS имя вашего домена. Если контроллер домена требует обязательной предварительной аутентификации, то необходимо вбить реквизиты пользователя имеющего права на доступ к Active Directory в поля Username и Password в файле C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml:

```
<init-param>
   <param-name>spnego.preauth.username</param-name>
   <param-value>Username</param-value>
</init-param>
<init-param>
```

```
        <param-name>spnego.preauth.password</param-name>
        <param-value>Password</param-value>
      </init-param>
```

- Убедиться, что для сервера приложений зарегистрирована SPN запись.

6. Настроить подключение приложения к БД. Для этого необходимо скопировать из Дистрибутива файл **properties_mssql_web** (или properties_oracle_web, в зависимости от используемой СУБД) в директорию **C:\Java\Tomcat7\conf**, изменить наименование скопированного файла на **properties**. В данном файле необходимо заменить в строке **bo.resource.docflow.connect** слова **SERVER** и **DATABASE** на сетевое имя сервера БД и наименование БД соответственно:

- для MSSQL:

```
bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://SERVER\:3436;databasename\=DATABASE\:tds\=8.0;lastupdatecount\=true
```

- для ORACLE:

```
bo.resource.DocFlow.connect=jdbc\:oracle\:thin\:@SERVER\:1521\:DATABASE
```

7. Скопировать файл **Application Server\jniwrap.dll** из дистрибутива в системный каталог **c:\Java\Tomcat7\bin**.
8. Переместить файл **C:\Java\Tomcat7\webapps\Docflow\WEB-INF\lib\jniwrap.jar** в каталог **c:\Java\Tomcat7\lib**.
9. Поместить на WEB сервер индивидуальный логотип организации. Для этого индивидуальный логотип **logo.jpg** следует записать в каталог ***C:\Java\Tomcat7\webapps\Docflow\images\main***.
10. Создать каталог для хранения временных файлов: **c:\TEMP.**
11. Убедиться в наличии файла **msvcr100.dll** в каталоге **c:\Windows\System32**, если его нет, то скопировать его в указанный каталог из дистрибутива Application Server\msvcr100.dll.
12. Запустить сервис Apache Tomcat Docflow с помощью менеджера служб Windows.
13. Для проверки правильности установки приложения Системы на WEB сервер, необходимо с любого компьютера, с которого разрешен доступ к данному серверу (по протоколу сетевого обмена http), в браузере Internet Explorer зайти по адресу **http://*server*/Docflow/security/logon.faces**, где *server* – сетевое имя компьютера - сервера приложений. В результате должна стать доступна стартовая страница приложения Системы.

4. Установка 64-бит версии сервера приложений Системы

Установка сервера приложений Системы должна выполняться на компьютере, выделенном под сервер приложений. Выполнять установку должен администратор Системы, с использованием файлов из каталога **Web** дистрибутива.

a.).

```
-XX:MaxPermSize=200m
-XX:+UseG1GC
-XX:+AggressiveOpts
-XX:+UseStringCache
-Djdk.map.althashing.threshold=0
-Duser.language=ru
-Duser.country=RU
-Dfile.encoding=cp1251
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.port=50000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.zirvan.properties=c:\Java\tomcat7\conf
```

b. При необходимости использования NTLM аутентификации в поле «Java Options» также требуется добавить следующую строку:

```
-Djcifs.properties=c:\Java\tomcat7\conf\jcifs.properties
```

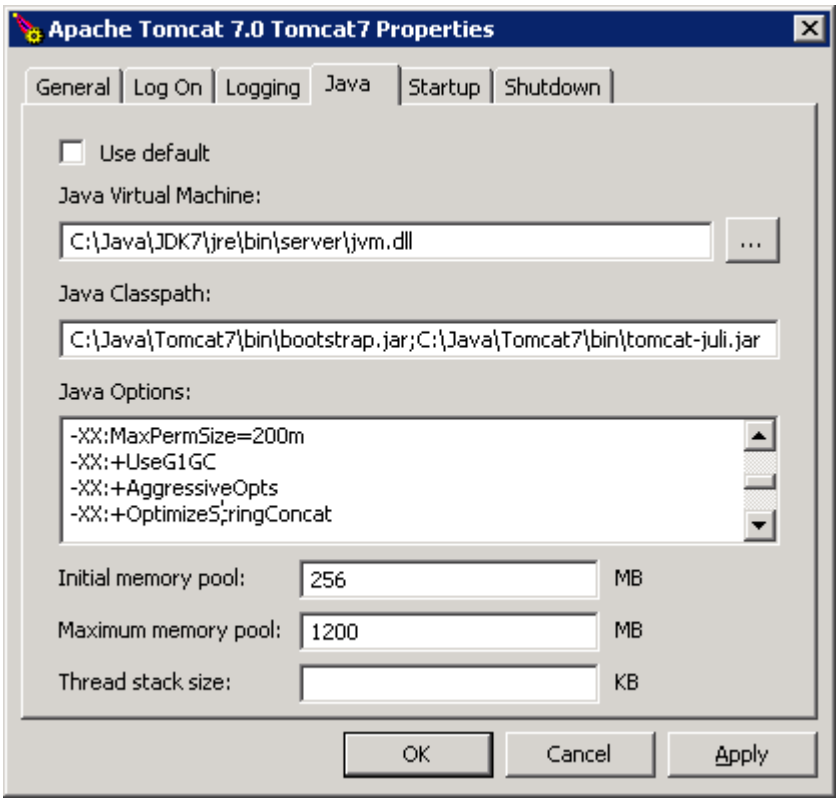


Рис. 3. Выбор количества оперативной памяти

4. В целях безопасности, необходимо отключить возможность удаленного управления, путем блокирования доступа к управляющим приложениям Tomcat с IP адресов отличных от localhost. Для этого в файле ***C:\Java\Tomcat7\webapps\manager\META-INF\context.xml*** тег Context заменяют на:

```
<Context antiResourceLocking="false" privileged="true">
        <Valve className="org.apache.catalina.valves.RemoteAddrValve"
               allow="127.0.0.1"/>
</Context>
```

5. На WEB сервере рекомендуется установить режим динамического сжатия данных, для чего следует скорректировать файл ***C:\Java\Tomcat7\conf****server.xml*, добавив в раздел нужного Connector'а следующие параметры:

```
compressionMinSize="2048"
noCompressionUserAgents="gozilla, traviata"
compressableMimeType="text/html,text/xml,text/javascript,text/css"
```

Пример (для типового случая, когда используется только стандартный Connector для порта 80):

```
<Connector port="80" protocol="HTTP/1.1" executor="tomcatThreadPool"
        connectionTimeout="20000"
        redirectPort="443"
        maxThreads="200"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="200"
        compression="on" compressionMinSize="2048" noCompressionUserAgents="gozilla,
traviata" compressableMimeType="text/html,text/xml"
        />
```

4.1. Установка прикладных модулей ядра Системы

В состав прикладных модулей ядра Системы, необходимых для работы, входят следующие модули:

- Модуль **jNotifier.Server**, предназначенный для доставки информационных сообщений получателю.
- Модуль **jScheduler.Server**, предназначенный для автоматического выполнения по расписанию пользовательских и служебных заданий.

Для установки этих модулей на сервере приложений необходимо запустить программу инсталлятора **DoXLogicServices_Setup.exe** из дистрибутива и следовать появляющимся на экране инструкциям.

6. По окончании процесса инсталляции появляется сообщение об успешном завершении.
7. Заменить конфигурационный файл **C:\Program Files\CSBI-Zirvan\DoXLogicServices\jScheduler.Server\properties** файлом из Дистрибутива **properties\properties_mssql_scheduler.** В новом файле **properties** отредактировать название Сервера БД и наименование БД:

```
bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://SERVER\:3436;databasename\=DATABASE\:tds\=8.0;l
astupdatecount\=true
```

8. Войти в управление службами ОС Windows, установить сервисы jNotifier.Server и jScheduler.Server в режим автоматического запуска и запустить их на выполнение.
9. Проверить корректность работы сервиса **jNotifier.Server**, для чего убедиться в наличии строки **«Notifier Service started»** в автоматически созданном файле протокола **not_out.txt** (см. каталог установки сервисов).
10. Проверить корректность работы сервиса **jScheduler.Server**, для чего убедиться в отсутствии строк **«error exception»** в автоматически созданном файле протокола **sched_out.txt** (см. каталог установки сервисов).

4.2. Установка приложения Системы на WEB - сервер

Публикация приложения Системы на компьютере сервера приложений осуществляется стандартным для Apache Tomcat способом. Ниже приводится описание порядка установки и начальной настройки приложения.

14. Остановить сервис Apache Tomcat DF с помощью менеджера служб Windows, если он был запущен.
15. Скопировать конфигурационный файл протоколирования **log4j.properties** из каталога properties инсталлятора в каталог ***C:\Java\Tomcat7\conf.***

16. Поместить файл **Web\Docflow.war** из дистрибутива Системы в каталог **C:\Java\Tomcat7\webapps.**

17. Для использования NTLM авторизации следует поместить файл jcifs.properties из дистрибутива в папку **C:\Java\Tomcat7\conf**. В нем нужно указать имя домена (заменив текст DOMAIN в приведенном ниже примере файла), на котором аутентифицируются пользователи Системы, и имя или IP адрес контроллера этого домена (заменив текст DOMAINCONTROLLER в приведенном ниже примере файла). Если контроллер домена требует обязательной предварительной аутентификации, то необходимо указать реквизиты пользователя имеющего права на доступ к Active Directory в поля USERNAME и PASSWORD.

```
jcifs.smb.lmCompatibility=0
jcifs.smb.client.useExtendedSecurity=false
# used when loadBalance=true
jcifs.smb.client.domain=DOMAIN
jcifs.util.loglevel=3
# if empty, will set loadBalance to true
jcifs.http.domainController=DOMAINONTROLLER
#jcifs.netbios.wins=WINSERVERIP1,WINSERVERIP1
jcifs.http.loadBalance=true
jcifs.smb.client.username=USERNAME
jcifs.smb.client.password=PASSWORD
jcifs.smb.client.soTimeout=400000
#jcifs.http.skipAuthList=127.0.0.1
```

Убедиться, что в политике безопасности домена разрешена NTLMv1 авторизация.

18. Для использования Kerberos авторизации (NTLMv2) необходимо:

- Отключить NTLM фильтр, если он был включен. Для этого требуется удалить файл C:\Java\Tomcat7\conf\jcifs.properties.
- После каждой установки обновления web-приложения системы ЭДО необходимо корректировать файл C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml. В нем необходимо раскомментировать тег «filter-mapping» для SPNEGO:

```
<filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
        <url-pattern>/security/*</url-pattern>
</filter-mapping>
```

- Скопировать из дистрибутива файлы krb5.conf и login.conf в каталог c:\Java\Tomcat7\conf, после чего в файле krb5.conf заменить все слова DOMAIN на NETBIOS имя вашего домена. Если контроллер домена требует обязательной предварительной аутентификации, то необходимо вбить реквизиты пользователя имеющего права на доступ к Active Directory в поля Username и Password в файле C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml:

```
<init-param>
  <param-name>spnego.preauth.username</param-name>
  <param-value>Username</param-value>
</init-param>
<init-param>
  <param-name>spnego.preauth.password</param-name>
  <param-value>Password</param-value>
</init-param>
```

- Убедиться, что для сервера приложений зарегистрирована SPN запись.

19. Настроить подключение приложения к БД. Для этого необходимо скопировать из Дистрибутива файл **properties_mssql_web** (или properties_oracle_web, в зависимости от используемой СУБД) в директорию **C:\Java\Tomcat7\conf**, изменить наименование скопированного файла на **properties**. В данном файле необходимо заменить в строке **bo.resource.docflow.connect** слова **SERVER** и **DATABASE** на сетевое имя сервера БД и наименование БД соответственно:

- для MSSQL:

```
bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://SERVER\:3436;databasename\=DATABASE\:tds\=8.0;lastupdatecount\=true
```

- для ORACLE:

bo.resource.DocFlow.connect=jdbc\:oracle\:thin\:@***SERVER***\:1521\:***DATABASE***

20. Скопировать файл **Application Server\jniwrap.dll** из дистрибутива в системный каталог **c:\Java\Tomcat7\bin**.
21. Переместить файл **C:\Java\Tomcat7\webapps\Docflow\WEB-INF\lib\jniwrap.jar** в каталог **c:\Java\Tomcat7\lib**.
22. Поместить на WEB сервер индивидуальный логотип организации. Для этого индивидуальный логотип **logo.jpg** следует записать в каталог ***C:\Java\Tomcat7\webapps\Docflow\images\main***.
23. Создать каталог для хранения временных файлов: **c:\TEMP.**
24. Убедиться в наличии файла **msvcr100.dll** в каталоге **c:\Windows\System32**, если его нет, то скопировать его в указанный каталог из дистрибутива Application Server\msvcr100.dll.
25. Запустить сервис Apache Tomcat Docflow с помощью менеджера служб Windows.
26. Для проверки правильности установки приложения Системы на WEB сервер, необходимо с любого компьютера, с которого разрешен доступ к данному серверу (по протоколу сетевого обмена http), в браузере Internet Explorer зайти по адресу **http://*server*/Docflow/security/logon.faces**, где *server* – сетевое имя компьютера - сервера приложений. В результате должна стать доступна стартовая страница приложения Системы.

5. Установка 64-бит версии сервера приложений Системы

Установка сервера приложений Системы должна выполняться на компьютере, выделенном под сервер приложений. Выполнять установку должен администратор Системы, с использованием файлов из каталога **Web** дистрибутива.

5.1. Установка JAVA-машины

Для работы сервера приложений Системы необходимо установить 64-бит версию JDK (Java SE Development Kit) версии 7. Ниже приведен порядок его установки:

7. Запустить инсталлятор **WEB\jdk-7u85-windows-x64.exe** из дистрибутива Системы, который установит следующее программное обеспечение:
   - Java SE Development Kit 7;

8. Во время инсталляции «Java SE Development Kit 7» необходимо изменить каталог установки «Development Tools» с предлагаемого по умолчанию адреса на **C:\Java\jdk64**, а также исключить «Public JRE» из набора предлагаемых для установки компонент, как показано на Рис. 1.

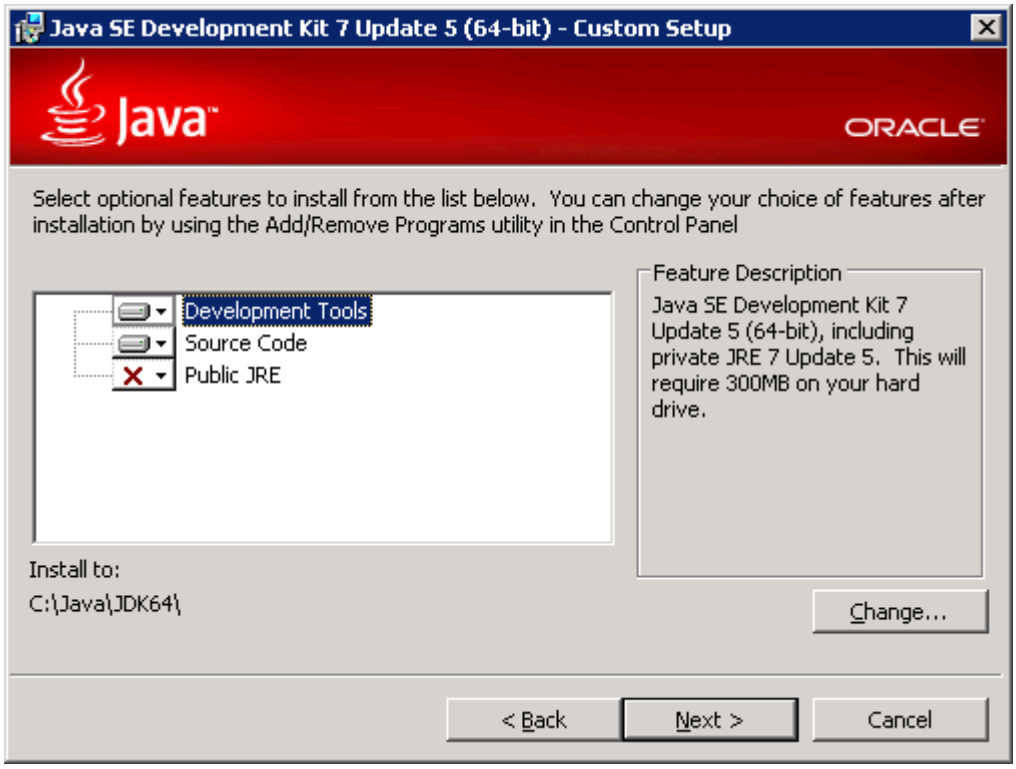


Рис. 4. Установка Java SE Development Kit 7

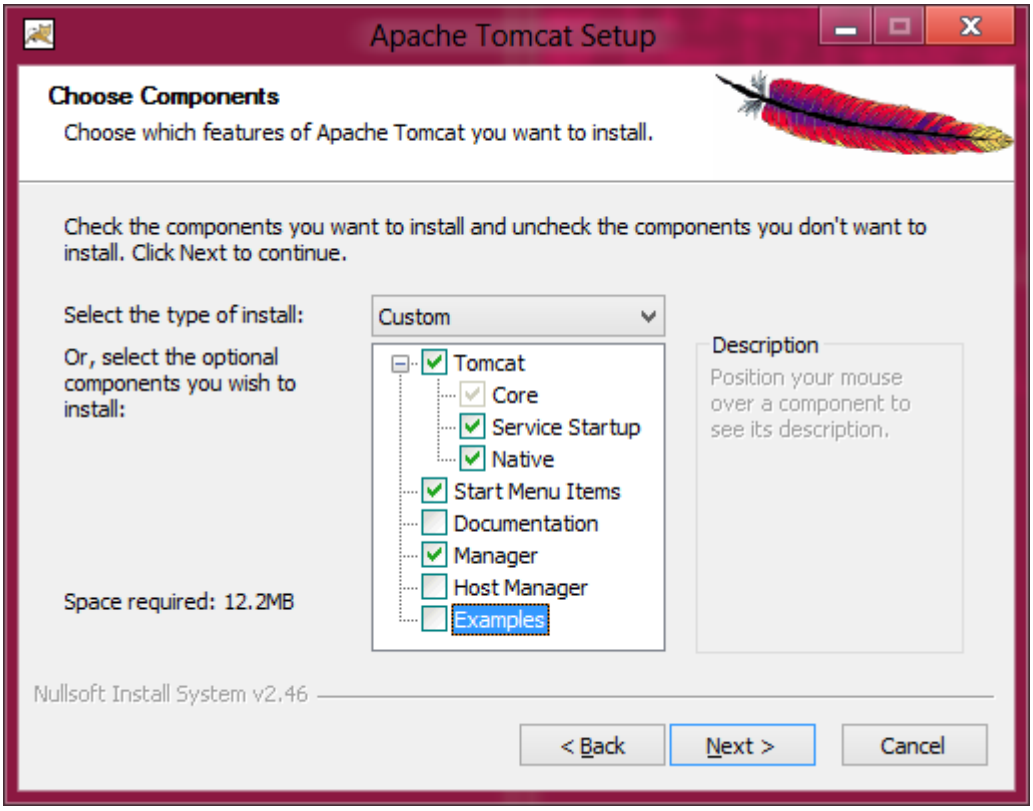
9. После нажатия на кнопку «Next» инсталлятор установит «Java SE Development Kit 7», после чего автоматически запуститься установка «JavaFX SDK», которую необходимо отменить.

10. По завершении процесса инсталляции на экране отобразится сообщение «**Installation Completed**» и будет запущен процесс регистрации, который можно пропустить.

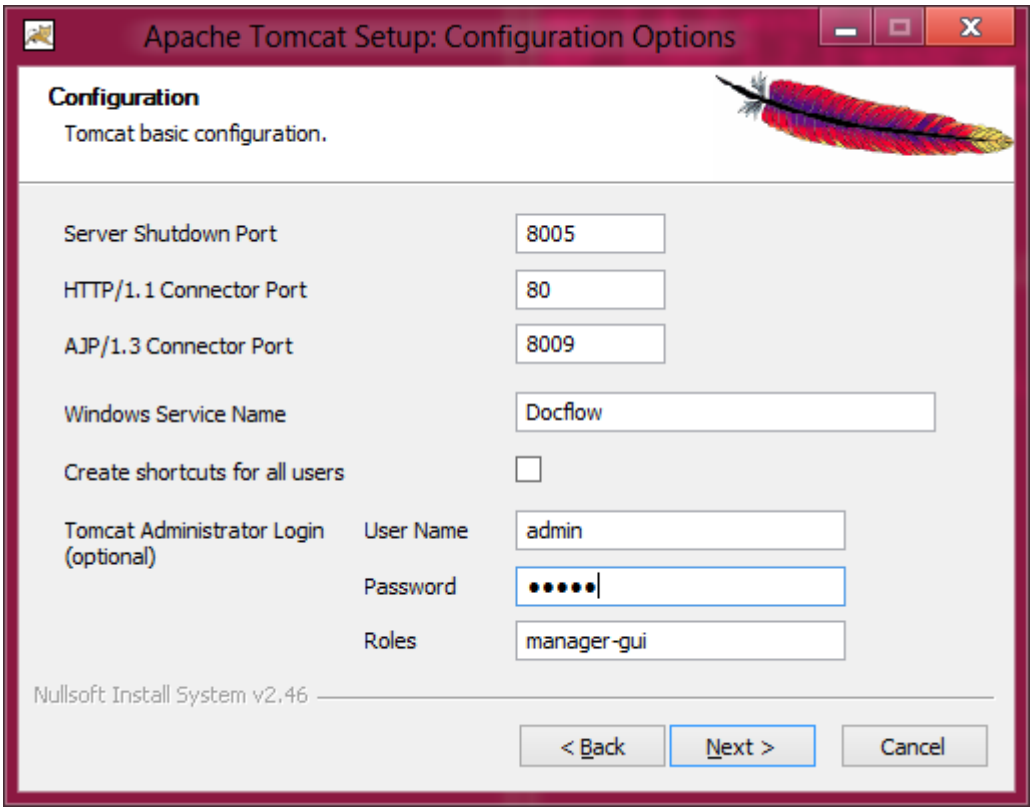
5.2. Установка сервера приложений «Application Server Tomcat»

1. Запустить инсталлятор из Дистрибутива **Web/apache-tomcat-7.0.68.exe**

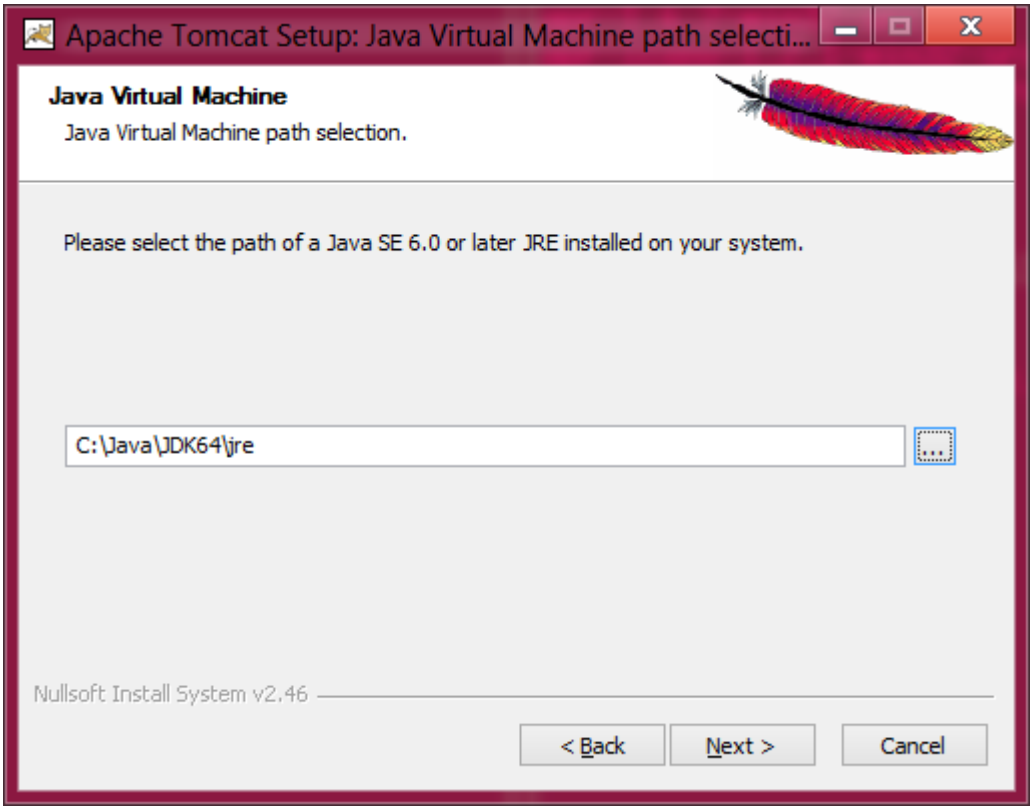
2. Выбрать необходимые компоненты, как на рисунке:



3. Указать порт, имя службы, логин и пароль администратора для Tomcat'а:



4. И указать путь к установленной JAVA Virtual Machine:



3. В качестве каталога для инсталляции укажите: **c:\Java\Tomcat64**

После установки Tomcat'а следует выполнить следующие операции:

1. Для обеспечения стабильной работы сервиса с большим количеством пользователей необходимо увеличить количество выделяемой сервису оперативной памяти. Для этого необходимо запустить окно настройки сервиса, выполнив последовательность действий:
   - **a.** Запустить созданный ярлык от имени администратора и выбрать закладку «Java»**;**
   - **b.** Убедиться, что поле «Java Virtual Machine» указывает на **c:\Java\jdk64\jre\bin\server\jvm.dll;**
   - c. В поле «Maximum memory pool» указать значение, равное объему памяти на сервере, в КБ, за вычетом 20%;
   - d. В поле «Java Options» добавить строчки, с обязательным сохранением дефисов: (см. Рис.6).

```
-XX:MaxPermSize=500m
-XX:+UseG1GC
-XX:MaxGCPauseMillis=500
-XX:+AggressiveOpts
-XX:+OptimizeStringConcat
-XX:+UseStringCache
-XX:+UseCompressedOops
-XX:+UseLargePages
-Djdk.map.althashing.threshold=0
-Duser.language=ru
-Duser.country=RU
-Dfile.encoding=cp1251
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.port=50000
-Dcom.sun.management.jmxremote.ssl=false
-Xloggc:c:\Java\gc.log
-XX:+PrintGCDetails
-XX:+PrintGCDateStamps
-Dcom.zirvan.properties=c:\Java\tomcat64\conf
```

e. При необходимости использования NTLM аутентификации в поле «Java Options» также требуется добавить следующую строку:

```
-Djcifs.properties=c:\Java\tomcat64\conf\jcifs.properties
```

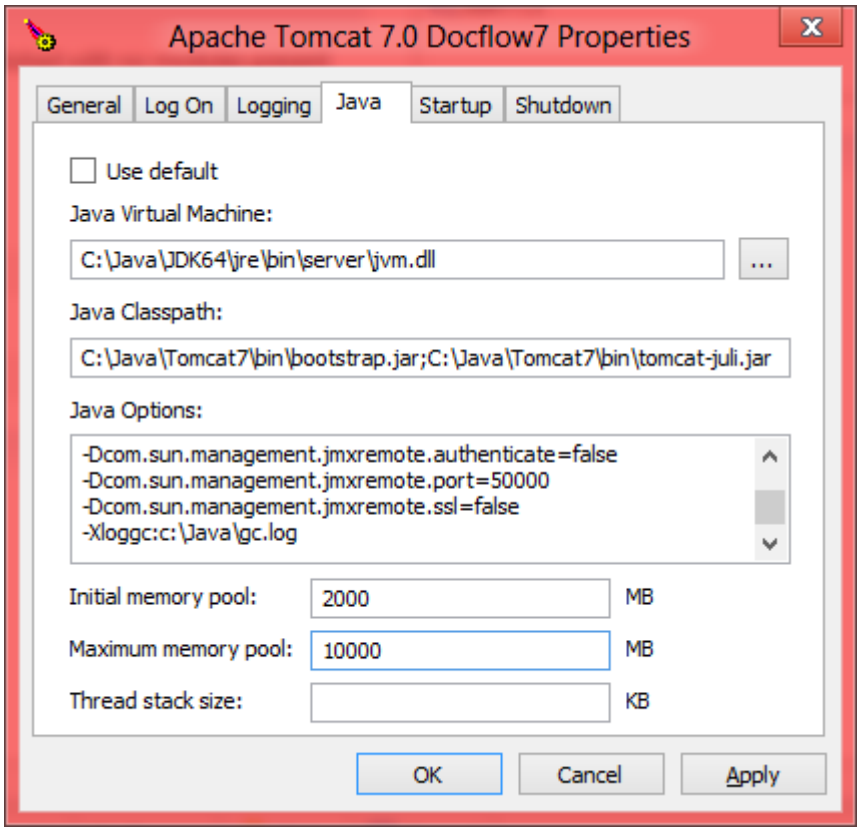


Рис. 5. Настройка виртуальной машины

2. В целях безопасности, необходимо отключить возможность удаленного управления, путем блокирования доступа к управляющим приложениям Tomcat с IP адресов отличных от localhost. Для этого в файле ***C:\Java\Tomcat64\webapps\manager\META-INF\context.xml*** тег Context заменяют на:

```
<Context antiResourceLocking="false" privileged="true">
        <Valve className="org.apache.catalina.valves.RemoteAddrValve"
               allow="127.0.0.1"/>
</Context>
```

3. Для проверки того, что сервер Apache Tomcat успешно установлен, необходимо запустить браузер MS Internet Explorer, зайти по адресу **http://localhost/** и убедиться, что страница «Apache Tomcat» успешно отобразилась.

5.3. Установка приложения Системы на WEB - сервер

Публикация приложения Системы на компьютере сервера приложений осуществляется стандартным для Apache Tomcat способом. Ниже приводится описание порядка установки и начальной настройки приложения.

1. Остановить сервис Apache Tomcat DF с помощью менеджера служб Windows.
2. Скопировать конфигурационный файл протоколирования **log4j.properties** из каталога properties инсталлятора в каталог ***C:\Java\Tomcat64\conf.***
3. Поместить файл **Web\Docflow.war** из дистрибутива Системы в каталог **C:\Java\Tomcat64\webapps**.
4. Для использования NTLM авторизации следует поместить файл jcifs.properties из дистрибутива в папку **C:\Java\Tomcat64\conf**. В нем нужно указать имя домена (заменив текст DOMAIN в приведенном ниже примере файла), на котором аутентифицируются пользователи Системы, и

имя или IP адрес контроллера этого домена (заменив текст DOMAINCONTROLLER в приведенном ниже примере файла). Если контроллер домена требует обязательной предварительной аутентификации, то необходимо указать реквизиты пользователя имеющего права на доступ к Active Directory в поля USERNAME и PASSWORD.

```
jcifs.smb.lmCompatibility=0
jcifs.smb.client.useExtendedSecurity=false
# used when loadBalance=true
jcifs.smb.client.domain=DOMAIN
jcifs.util.loglevel=3
# if empty, will set loadBalance to true
jcifs.http.domainController=DOMAINONTROLLER
#jcifs.netbios.wins=WINSERVERIP1,WINSERVERIP1
jcifs.http.loadBalance=true
jcifs.smb.client.username=USERNAME
jcifs.smb.client.password=PASSWORD
jcifs.smb.client.soTimeout=400000
#jcifs.http.skipAuthList=127.0.0.1
```

Убедиться, что в политике безопасности домена разрешена NTLMv1 авторизация.

5. Для использования Kerberos авторизации (NTLMv2) необходимо:

   - Отключить NTLM фильтр, если он был включен. Для этого требуется удалить файл C:\Java\Tomcat7\conf\jcifs.properties.
   - После каждой установки обновления web-приложения системы ЭДО необходимо корректировать файл C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml. В нем необходимо раскомментировать тег «filter-mapping» для SPNEGO:

```
<filter-mapping>
<filter-name>SpnegoHttpFilter</filter-name>
        <url-pattern>/security/*</url-pattern>
</filter-mapping>
```

   - Скопировать из дистрибутива файлы krb5.conf и login.conf в каталог c:\Java\Tomcat7\conf, после чего в файле krb5.conf заменить все слова DOMAIN на NETBIOS имя вашего домена. Если контроллер домена требует обязательной предварительной аутентификации, то необходимо вбить реквизиты пользователя имеющего права на доступ к Active Directory в поля Username и Password в файле C:\Java\Tomcat7\webapps\Docflow\WEB-INF\web.xml:

```
<init-param>
   <param-name>spnego.preauth.username</param-name>
   <param-value>Username</param-value>
</init-param>
<init-param>
   <param-name>spnego.preauth.password</param-name>
   <param-value>Password</param-value>
</init-param>
```

   - Убедиться, что для сервера приложений зарегистрирована SPN запись.

6. Настроить подключение приложения к БД. Для этого необходимо скопировать из Дистрибутива файл **properties_mssql_web** (или properties_oracle_web, в зависимости от используемой СУБД) в директорию **C:\Java\Tomcat64\conf**, изменить наименование скопированного файла на **properties**. В данном файле необходимо заменить в строке **bo.resource.docflow.connect** слова **SERVER** и **DATABASE** на сетевое имя сервера БД и наименование БД соответственно:

   - для MSSQL:

```
bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://SERVER\:3436;databasename\=DATABASE\:tds\=8.0;lastupdatecount\=true
```

   - для ORACLE:

```
bo.resource.DocFlow.connect=jdbc\:oracle\:thin\:@SERVER\:1521\:DATABASE
```

7. Создать каталог для хранения временных файлов: **c:\TEMP.**
8. Запустить сервис Apache Tomcat с помощью менеджера служб Windows.

9. Для проверки правильности установки приложения Системы на WEB сервер, необходимо с любого компьютера, с которого разрешен доступ к данному серверу (по протоколу сетевого обмена http), в браузере Internet Explorer зайти по адресу **http://*server*/Docflow/**, где *server* – сетевое имя компьютера - сервера приложений. В результате должна стать доступна стартовая страница приложения Системы.

5.4. Установка прикладных модулей ядра Системы

В состав прикладных модулей ядра Системы, необходимых для работы, входят следующие модули:

- Модуль **jNotifier.Server**, предназначенный для доставки информационных сообщений получателю.
- Модуль **jScheduler.Server**, предназначенный для автоматического выполнения по расписанию пользовательских и служебных заданий.

Для установки этих модулей на сервере приложений необходимо запустить программу инсталлятора **DoXLogicServices_Setup.exe** из дистрибутива и следовать появляющимся на экране инструкциям.

11. По окончании процесса инсталляции появляется сообщение об успешном завершении.
12. Заменить конфигурационный файл **C:\Program Files\CSBI-Zirvan\DoXLogicServices\jScheduler.Server\properties** файлом из Дистрибутива **properties_mssql_scheduler** (или properties_oracle_scheduler, в зависимости от используемой СУБД)**.** В новом файле **properties** необходимо заменить в строке **bo.resource.docflow.connect** слова **SERVER** и **DATABASE** на сетевое имя сервера БД и наименование БД соответственно:
    - для MSSQL:

bo.resource.docflow.connect=jdbc\:jtds\:sqlserver\://***SERVER***\:3436;databasename\=***DATABASE***\:tds\=8.0;lastupdatecount\=true

    - для ORACLE:

bo.resource.DocFlow.connect=jdbc\:oracle\:thin\:@***SERVER***\:1521\:***DATABASE***

13. Войти в управление службами ОС Windows, установить сервисы jNotifier.Server и jScheduler.Server в режим автоматического запуска и запустить их на выполнение.
14. Убедиться в наличии файла **msvcr71.dll** в каталоге **c:\Windows\System32**, если его нет, то скопировать его в указанный каталог из дистрибутива **Application Server\msvcr71.dll** и в каталог **c:\Windows\SysWOW64**).
15. Проверить корректность работы сервиса **jNotifier.Server**, для чего убедиться в наличии строки **«Notifier Service started»** в автоматически созданном файле протокола **not_out.txt** (см. каталог установки сервисов).
16. Проверить корректность работы сервиса **jScheduler.Server**, для чего убедиться в отсутствии строк **«error exception»** в автоматически созданном файле протокола **sched_out.txt** (см. каталог установки сервисов).

6. Настройка HTTPS подключения к серверу Системы

Данный раздел содержит инструкции по настройке сервера Apache Tomcat для обеспечения защищенного обмена данными на основе SSL.

После выполнения перечисленных в документе настроек, сервер Tomcat будет работать следующим образом: если приложению соответствует адрес «http://сервер:8080/Docflow», то все запросы, направленные по этому адресу, будут автоматически перенаправлены на шифрованное SSL соединение по адресу «https://сервер:8443/Docflow».

В зависимости от политики безопасности организации, в приложении можно использовать сертификаты, полученные из официальных источников или сформированные самостоятельно. В данном документе рассматривается вариант самостоятельного создания сертификатов.

Для того, чтобы Tomcat мог обрабатывать запросы по шифрованным соединениям, необходимо выполнить следующие действия:

- Сформировать сертификаты, которые будут использоваться при шифровании.
- Настроить сервер Tomcat.
- Указать в настройках приложения необходимость работы только по защищенному SSL соединению.

Важно! *После настройки шифрованного подключения необходимо выполнить на всех рабочих местах пользователей настройку, описанную в пункте 8 раздела 6.1.*

6.1. OpenSSL

Для выполнения данной настройки потребуется сгенерировать ключи и сертификаты при помощи программного обеспечения OpenSSL, входящего в комплект инсталлятора Системы.

Ниже приведено описание процедуры формирования «самоподписанного» сертификата сервера. Для получения сертификата сервера, заверенного официальным CA, необходим запрос на получение сертификата, формирование которого описано в пункте 5, при этом пункты 1-4 и 6 выполнять не следует.

1. Создание закрытого ключа и запроса на сертификат для собственного CA

```
openssl req -new -config openssl.cnf -newkey rsa:1024 -nodes -out ca.csr -keyout
ca.key
```

2. Создание сертификата для собственного CA:

```
openssl x509 -trustout -signkey ca.key -days 1001 -req -in ca.csr -out ca.pem
```

`1001` – количество дней действия сертификата

3. Если скопировать файл ca.pem в ca.crt, изменить внутреннее содержимое, чтобы фраза “TRUSTED CERTIFICATE” читалась как “ CERTIFICATE”, этот файл можно импортировать в Windows и установить его в хранилище доверенных корневых сертификатов:

```
echo -----BEGIN CERTIFICATE----- > ca.crt
findstr /V " TRUSTED " ca.pem >> ca.crt
echo -----END CERTIFICATE----- >> ca.crt
```

4. Создание файла серийных номеров для собственного CA:

```
echo 02 > ca.srl
```

5. Создание закрытого ключа и запроса на сертификат для Web-сервера:

```
openssl req -new -config openssl.cnf -newkey rsa:1024 -nodes -out server.csr -
keyout server.key
```

6. Создание сертификата для сервера на основе запроса при помощи собственного CA. Этот этап необходимо пропустить, если требуется иметь сертификат сервера, заверенный официальным CA.

```
openssl x509 -CA ca.pem -CAkey ca.key -CAserial ca.srl -req -in server.csr -out server.crt -days 1001
```

`1001` – количество дней действия сертификата

Файлы server.crt и server.key, полученные в результате этих действий, необходимо поместить в директорию ***c:\Java\Tomcat\conf*** .

Конфигурирование коннекторов осуществляется правкой конфигурационного файла server.xml, находящегося в подкаталоге conf рабочей директории Tomcat.

- Необходимо убедиться в наличии и активности атрибута redirectPort="8443" в теге Connector, соответствующем нешифрованным соединениям (по умолчанию на порт 8080);
- В тег Connector, соответствующий шифрованным соединениям (по умолчанию на порт 8443), необходимо добавить ссылки на полученные сертификат и ключ (атрибуты SSLCertificateFile="${catalina.base}/conf/server.crt" и SSLCertificateKeyFile="${catalina.base}/conf/server.key"), а также убедиться, что данный тег не закомментирован.

```
<Connector port="443" maxHttpHeaderSize="8192"
           maxThreads="150"
           enableLookups="false" disableUploadTimeout="true"
           acceptCount="100" scheme="https" secure="true"
           SSLEnabled="true"
           SSLCertificateFile="${catalina.base}/conf/server.crt"
           SSLCertificateKeyFile="${catalina.base}/conf/server.key" />
```

6.2. КриптоПро JCP/JTLS

Инструкция по установке и настройке КриптоПро JCP и КриптоПро JTLS (версии 1.0.47) для работы с web-сервером Apache Tomcat 7.

Инструкция составлена к следующей начальной конфигурации:
Установлен JDK1.7 в каталог C:\ Java\jdk64.
Установлен Tomcat 7.x в каталог C:\Java\Tomcat64.
Для другой начальной конфигурации надо исправить в инструкции соответствующие пути к файлам.
Для установки необходимо предварительно получить серверные лицензии для продуктов КриптоПРО JCP и КриптоПРО JTLS, иначе будет ограничение по времени работы.

Необходимые файлы:

- JCP.1.0.47.zip
- JTLS.1.0.47.zip
- local_policy.jar - версия файла без экспортных ограничений
- makeGostTLSkey.jar (программа генерации серверного ключа и сертификата)
- ca.cer - сертификат удостоверяющего центра, которым подписывается сертификат сервера

Пошаговая инструкция:

- Разархивировать файл JCP.1.0.47.zip в каталог Java\CryptoPro\JCP
- Разархивировать файл JTLS.1.0.47.zip в каталог Java\CryptoPro\JTLS
- Скопировать local_policy.jar в каталог Java\jdk64\jre\lib\security , заменив оригинальный файл с тем же именем.
- Запустить командный интерпретатор (cmd или Far) от имени администратора.
- Установить в качестве текущего каталог Java\CryptoPro\JCP\lib и выполнить команду:

install C:\Java\jdk64\jre XXXXX-XXXXX-XXXXX-XXXXX-XXXXX "Имя Компании"

первый аргумент – путь к каталогу jre внутри JDK
второй аргумент – номер лицензии КриптоПро JCP
третий аргумент – имя компании, которой выдана лицензия.

Если второй и третий аргументы не указаны, то устанавливается демо-версия, но номер лицензии и имя компании можно ввести позднее через панель управления JCP (см.ниже).

После выполнения команды необходимо убедиться, что появилось сообщение об успешной установке на англ. языке.

- Установить в качестве текущего каталог Java\CryptoPro\JTLS\lib и выполнить:

c:\Java\jdk64\bin\java -cp cpSSL.jar ru.CryptoPro.ssl.JTLSInstall -install -verbose -sslserial XXXXX-XXXXX-XXXXX-XXXXX-XXXXX -sslcompany "Имя Компании"

(здесь используется номер лицензии для КриптоПРО JTLS, который не совпадает с номером лицензии для JCP). Аналогично, номер лицензии и имя компании можно ввести позднее через контрольную панель JCP.

- Скопировать из текущего каталога (Java\CryptoPro\JTLS\lib) файл TomcatSSL.jar в каталог, где хранятся библиотеки, подключаемые к Tomcat (Java\Tomcat6\lib).
- Перейти в каталог Java\CryptoPro\JCP\lib и запустить панель управления JCP при помощи команды:

ControlPane.bat c:\Java\jdk64\jre
Выбрать вкладку «Оборудование» и установить «Путь к хранилищу HDImage»:
C:\Java\CryptoPro\HDImageStore
В этот каталог будет записан сгенерированный ключ.

- Создать ключ и сертификат при помощи программы makeGostTLSkey. Для этого поместить в какой-либо каталог файлы makeGostTLSkey.jar и ca.cer и запустить в нем команду:

c:\Java\jdk64\bin\javaw –jar makeGostTLSkey.jar

В открывшемся окне заполнить необходимые поля, причем в поле 'CN= ‘ должно быть указано доменное имя сервера, на котором работает Tomcat. В поле Password надо указать пароль доступа к хранилищу ключа, тот же самый пароль должен быть указан в настройках SSL-коннетора (см. дальше). В поле CA URL должен быть указан URL Удостоверяющего Центра, через который происходит выдача сертификата. Это значение инициализировано тестовым УЦ Крипто-Про. Если это поле будет пустым, то создается самоподписанный сертификат. После заполнения полей следует нажать на кнопку «Создать», появится окно для рандомизации процесса генерации ключа, после отображения которого надо подвигать мышкой произвольным образом. После этого ключ и сертификат будут сохранены в хранилище HDImageStore, кроме того копия полученного сертификата будет помещена в файл ssl.cer, а также будет создан файл tomcat.keystore. Файл tomcat.keystore надо скопировать в каталог c:\Java\Tomcat64\conf

- Настроить ssl-коннектор в файле Java\Tomcat64\conf\server.xml:

```
<Connector port="8443" maxHttpHeaderSize="8192"
           protocol="org.apache.coyote.http11.Http11Protocol"
           acceptCount="10"
           enableLookups="false" disableUploadTimeout="true"
           maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
           SSLEnabled="true"
           scheme="https" secure="true"
           clientAuth="false"
           sslProtocol="GostTLS"
           algorithm="GostX509"
           keyalg="GOST3410"
           sigalg="GOST3411withGOST3410EL"
           keystoreProvider="JCP"
           keystoreFile="${catalina.base}/conf/tomcat.keystore"
           keystorePass="zirvan"
           keystoreType="HDImageStore"
           keystoreAlias="tomcat"
           SSLImplementation="ru.CryptoPro.TomcatSSL.JSSEImplementation" />
```

7. Установка клиентской части системы на рабочие места пользователей

7.1. Для WEB-приложения

Для установки WEB-модуля приложения Системы на рабочих компьютерах пользователей нужно выполнить следующие шаги:

1. Убедится, что на компьютере установлен браузер MS Internet Explorer версии 8.0 SP1 либо выше.
2. Установить ПО Java Runtime Environment 7.0 (сокр. JRE) (последнюю версию можно бесплатно скачать с сайта-разработчика JRE по следующему адресу: http://www.java.com/en/download/).
3. В свойствах браузера Internet Explorer открыть закладку «Безопасность» (в английской версии – «Security»), перейти на закладку «Разрешенные Узлы» («Trusted sites»), нажмите на кнопку «Узлы» («Sites»), после чего добавить сетевое имя WEB-сервера Системы в список разрешенных. Если защищенное соединение не используется, то следует отключить признак поддержки https:

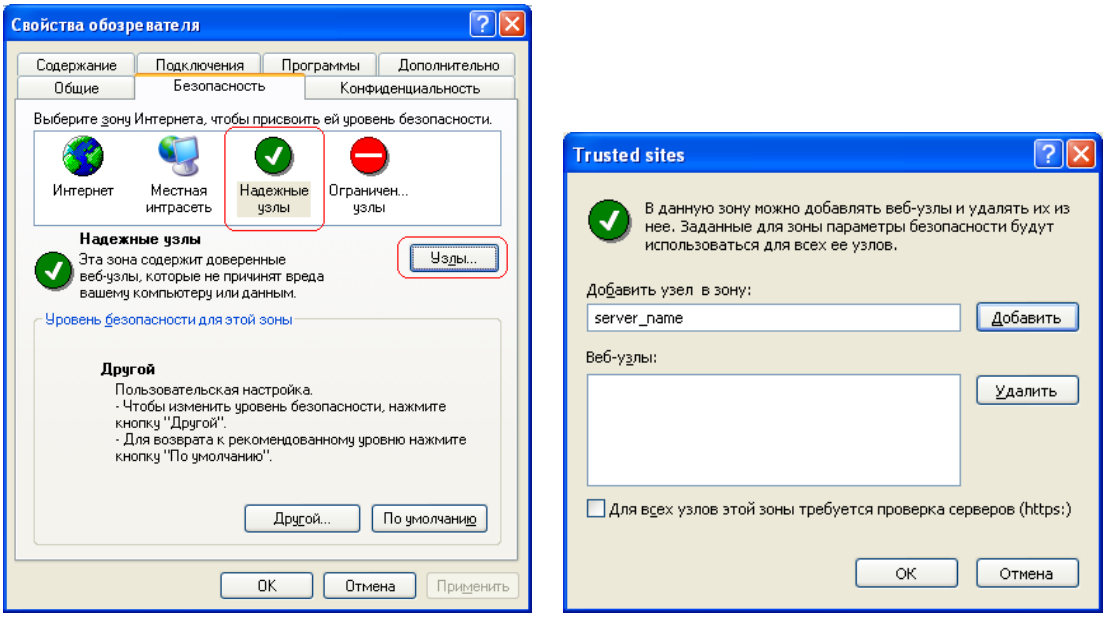


Рис. 1. Настройка разрешения доступа в браузере

Далее следует настроить уровень безопасности при работе с доверенными узлами. Для этого надо понизить уровень безопасности до Низкого, а затем нажать Другой («Custom Level») на форме свойств браузера.

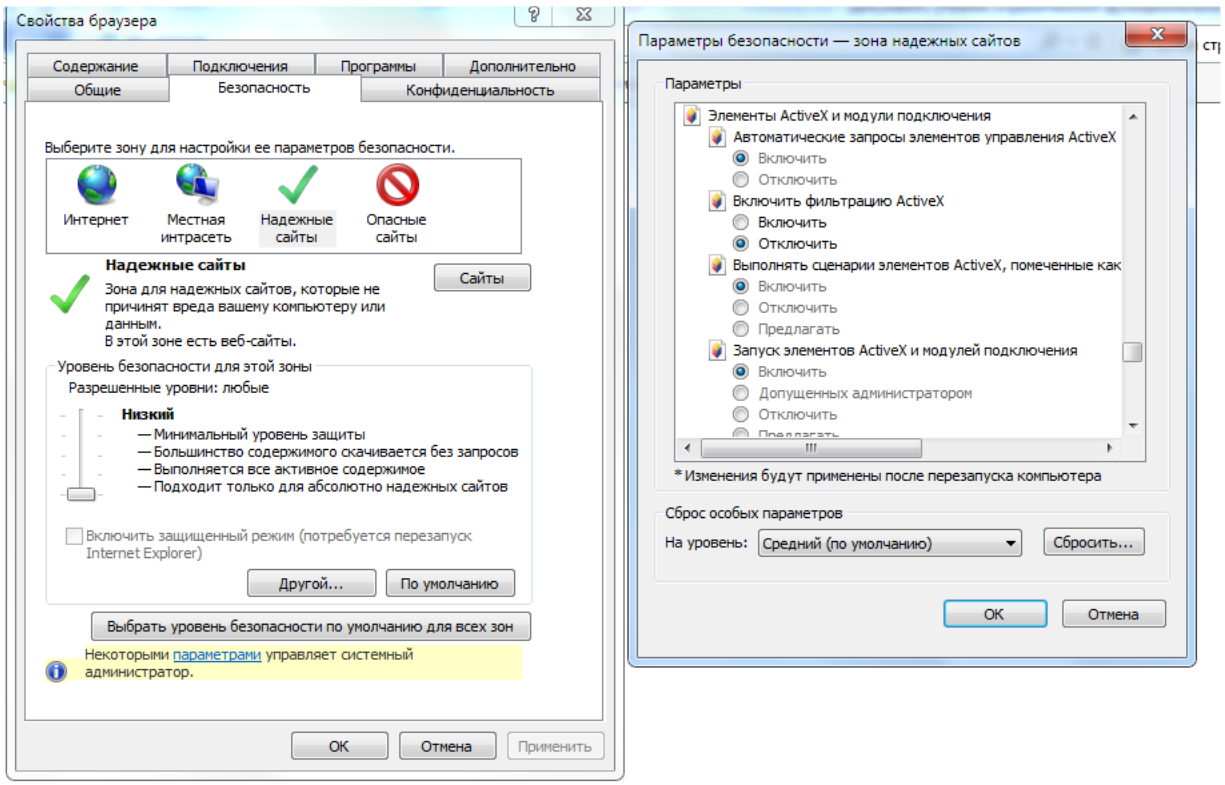


Рис. 2. Настройка уровня безопасности браузера

В появившемся перечне проверить, что разрешение «Включить» стоит для следующих параметров:

- Выполнять сценарии ActiveX, помеченные как безопасные
- Запускать элементы ActiveX и модулей
- Использовать элементы управления ActiveX, не помеченных как безопасные
- Разрешить запуск элементов управления ActiveX, которые не использовались ранее
- Скачать подписанные элементы ActiveX
- Скачать неподписанные элементы ActiveX

4. В свойствах браузера Internet Explorer открыть закладку «Содержание» («Content»), нажать на кнопку «Автозаполнение» («AutoComplete») и включить признак «Форм» («Forms») (**Ошибка! Неверная ссылка закладки.**3).

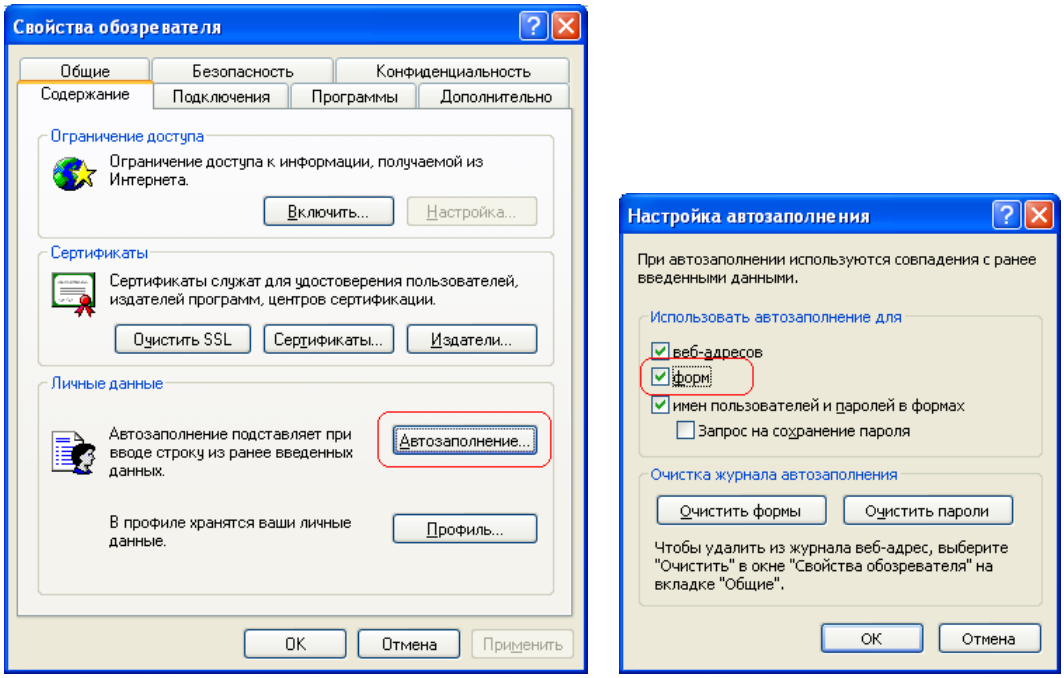


Рис.3. Настройка автозаполнения

5. Необходимо выполнить следующие настройки:

5.1. Открыть Пуск – Все программы – Java – Configure Java. В открывшемся окне нажать Manage certificates

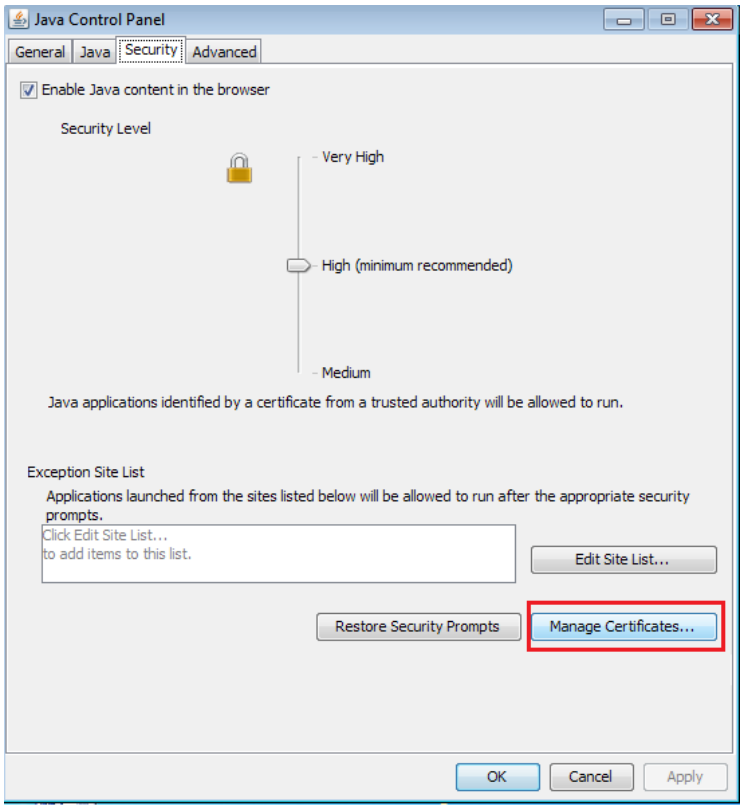


Рис.4. Открытие настроек Java

5.2. Выбрать тип сертификата Signer CA, нажать Import

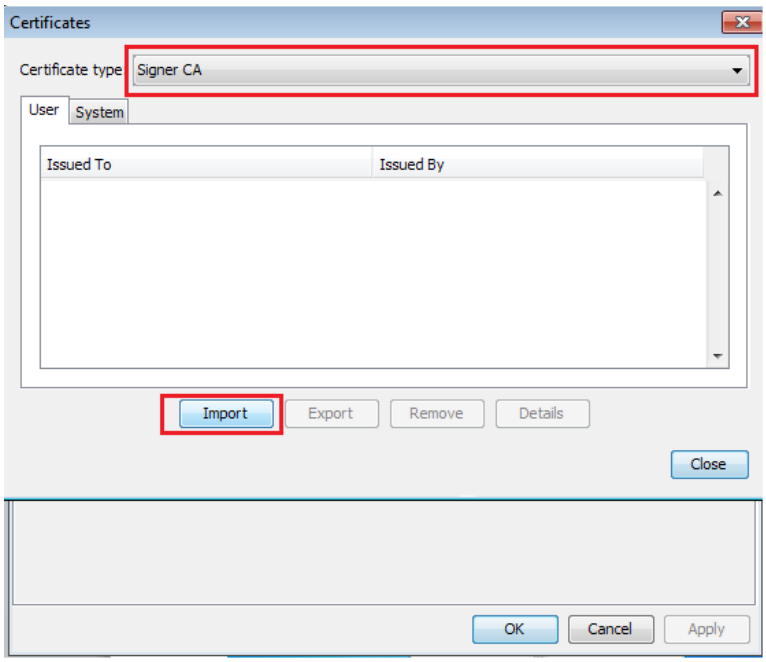


Рис 5. Выбор типа сертификата

5.3. Выбрать тип файлов All files, сертификат ZirvanrootCA, нажать Open – OK. (сертификат находится в папке WEB комплекта инсталлятора).

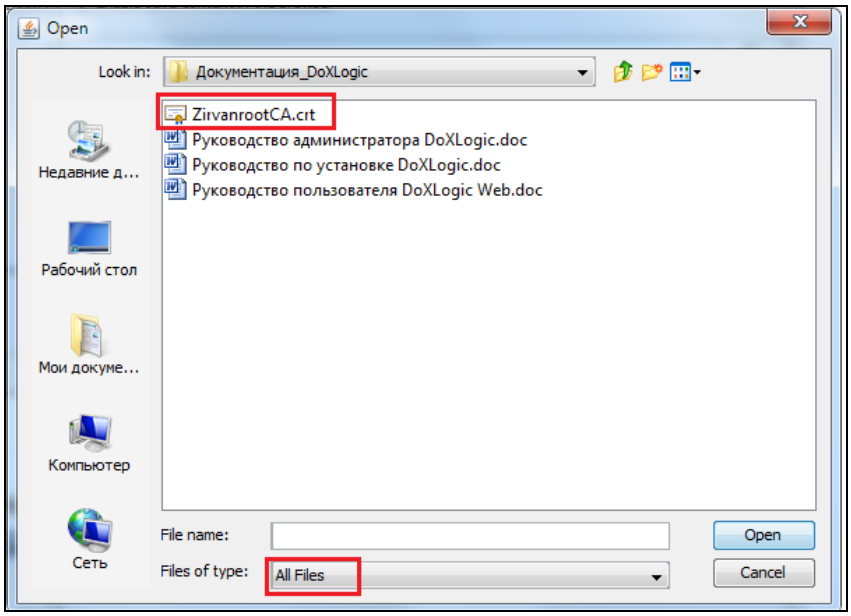
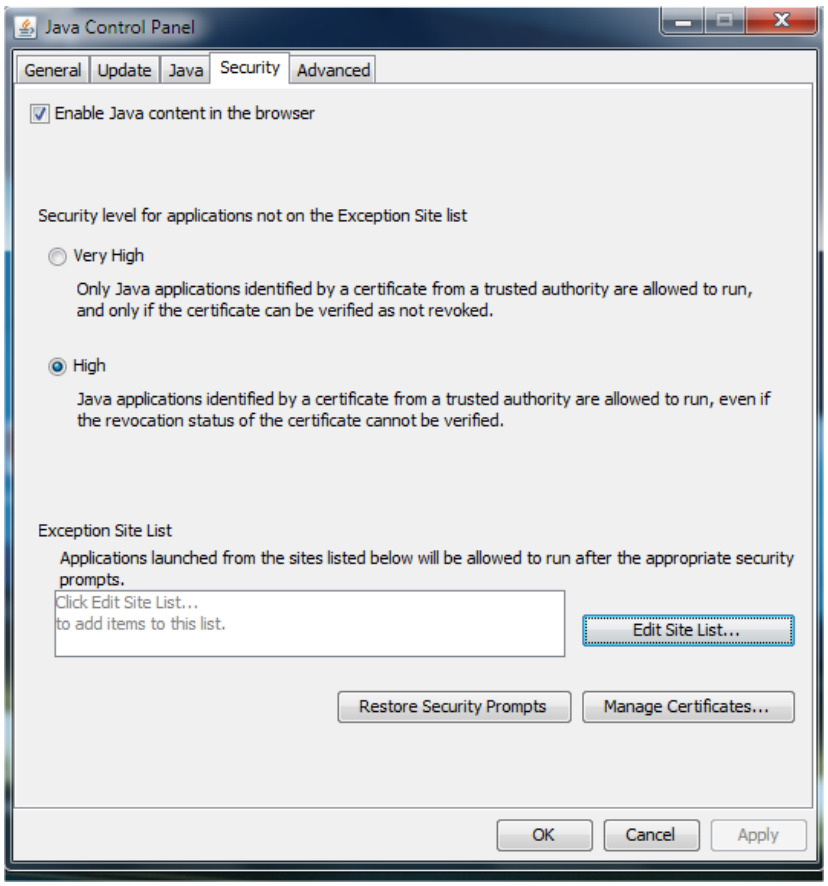
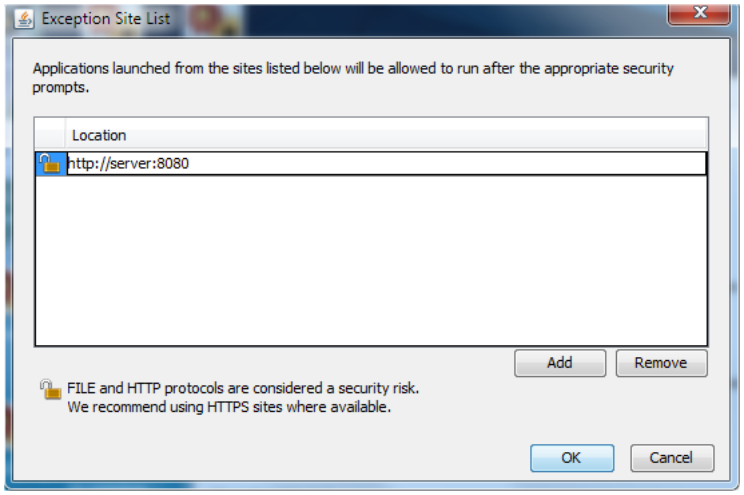


Рис 6. Выбор сертификата

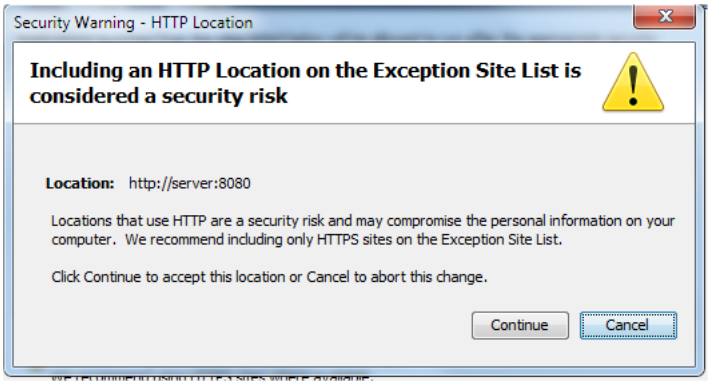
5.4. Открыть Все программы – Java – Configure Java – Security – Edite site list



5.5. В открывшемся окне добавить URL приложения (с указанием порта при наличии, без указания наименования приложения) например, http://server:8080. Нажать Ok.



5.6. В появившемся окне нажать Continue



5.7. Зайти в форму множественного прикрепления документов в Web-приложении. В появившемся окне ставим галочку и нажимаем Run:

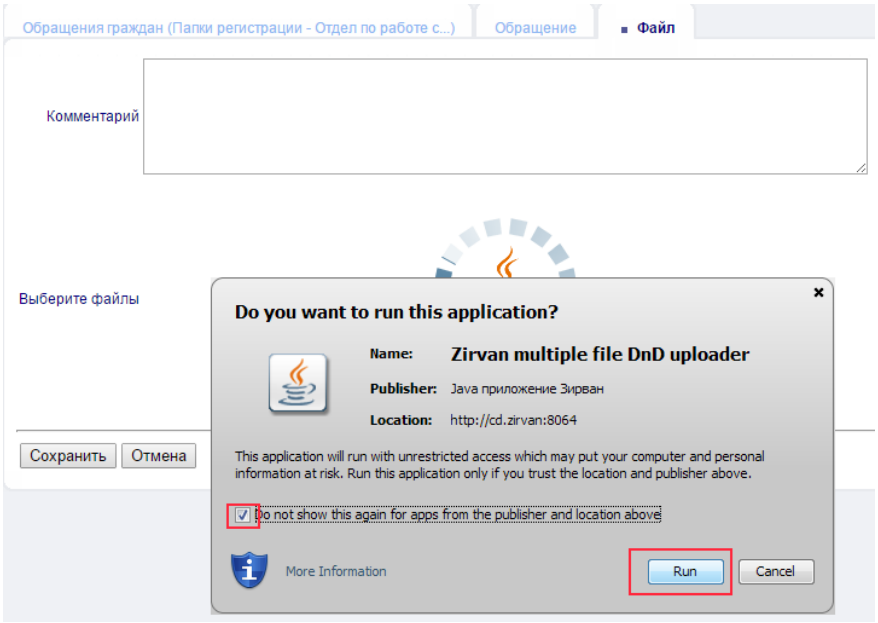


Рис 7. Проставление галочки

5.8. Добавить документы, в появившемся окне поставить галочку и нажать Allow:

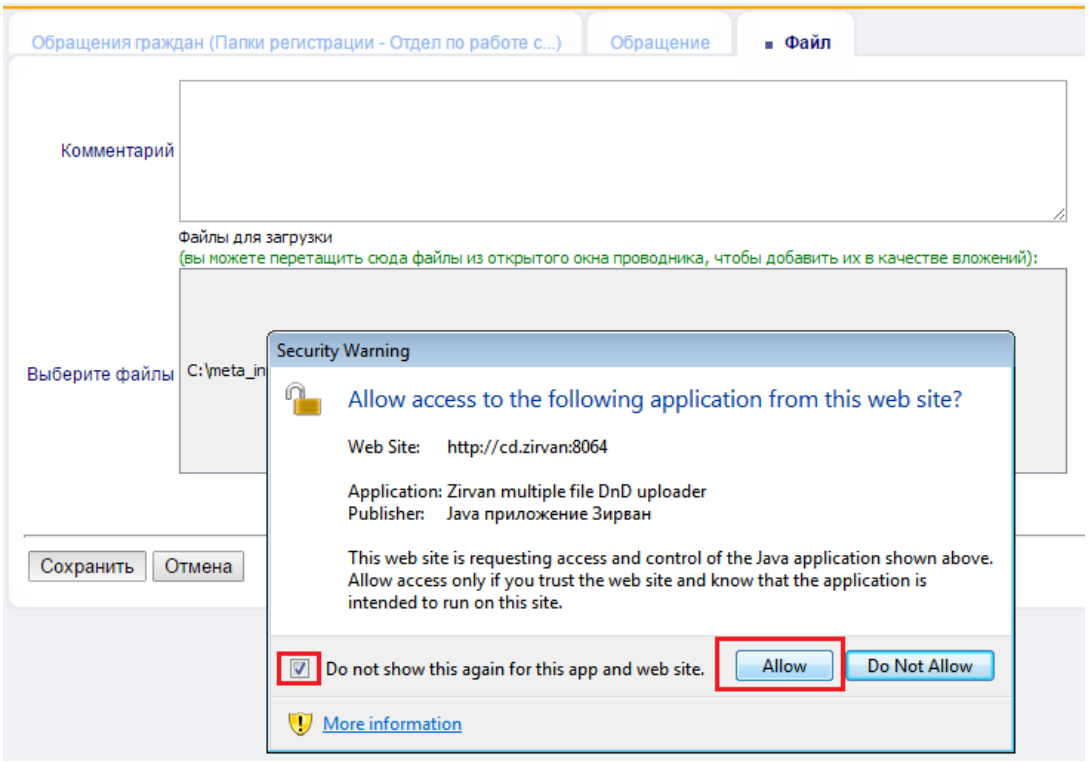


Рис.8. Проставление галочки

6. Для работы с приложением Системы поместить в «Избранное» следующую ссылку **http://*server*:8080/DocflowWeb/security/logon.faces**, где *server* – сетевое имя компьютера – сервера приложений Системы.
7. Для работы функционала ЭЦП необходимо установить соответствующую библиотеку **Web/capicominst.rar**.
8. Для корректной работы отчета «Печать конверта» на рабочую станцию пользователя установить шрифт из файла дистрибутива zipcode.TTF.
9. В связи с официально зафиксированным компанией Microsoft «бага» в Internet Explorer версий 6-8 (http://support.microsoft.com/kb/323308 Код статьи: 323308 - Последнее изменение: 24 ноября 2010 г. - Редакция: 3.0, http://support.microsoft.com/kb/815313), который приводит к ошибкам загрузки (download) файлов при включенном SSL протоколе, необходимо установить на рабочие места пользователей рекомендуемое компанией Microsoft обновление (добавление ключа в реестр). Для упрощения выполнения данной задачи необходимо разослать пользователям ЭДО самоустанавливающийся файл BypassSSLNoCacheCheck_User.reg (содержание файла см. ниже) с указанием его открыть (например, двойным кликом мыши). Для выполнения этого действия пользователю не обязательно обладать правами администратора.

   Содержание файла BypassSSLNoCacheCheck_User.reg :

   Windows Registry Editor Version 5.00

   [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

   "BypassSSLNoCacheCheck"=dword:00000001
10. Для информации: в браузере Chrome версии 42 (и более новых) по умолчанию запрещены java applets. Т.е. не работает множественная загрузка и редактирование файлов. Чтобы их включить, надо включить флаг {{chrome://flags/#enable-npapi}}. Для этого в адресной строке браузера набрать chrome://flags/#enable-npapi и нажать <Enter>. После чего в появившемся окне нажать кнопку «Включить» (см. Рис.9)

    В Chrome версии 45 и выше данная функция была упразднена.

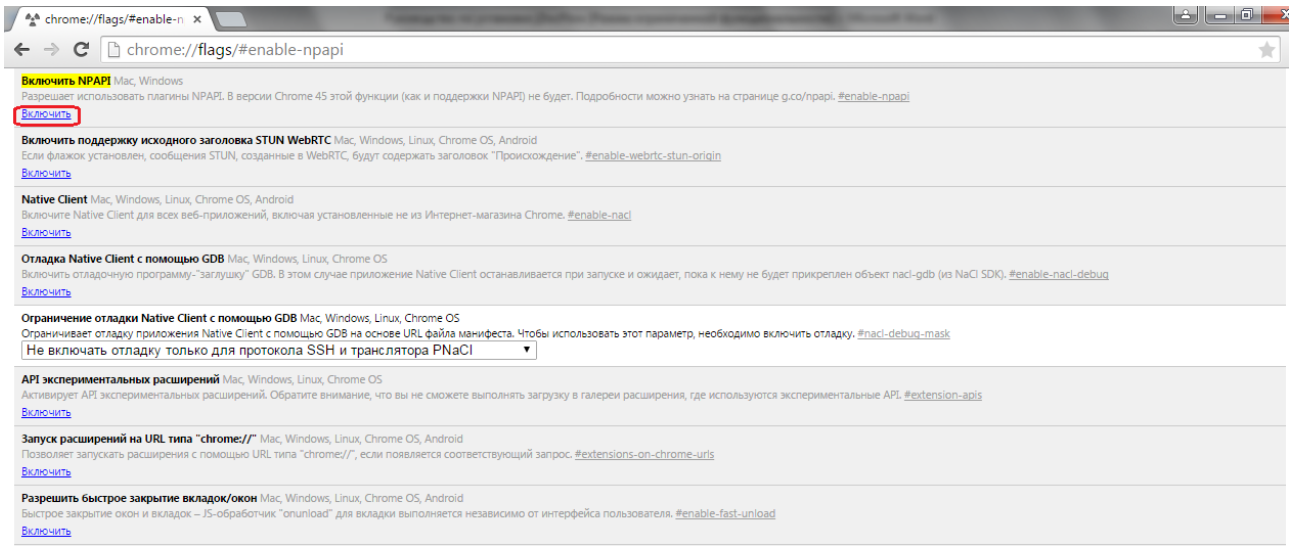


Рис.9. Настройка браузера Chrome

7.2. Для desktop-приложения (при работе пользователей через толстый клиент)

Настройка файлового ресурса

Данные подготовительные работы по установке клиентской части desktop-приложения должен выполнять администратор Системы (с использованием файлов из корневого каталога дистрибутива).

1. Организовать на любом файловом сервере ресурс (каталог) с именем **DocflowDesktop**, доступный для чтения всем пользователям desktop-приложения Системы.
2. Разархивировать в этот каталог, с помощью стандартных средств MS Windows файлы **jAll_Desktop.rar** из дистрибутива.
3. В файле **DocflowDesktop\properties** в следующей строке заменить строку SERVER на сетевое имя сервера приложения Системы (см. раздел 4.2):

```
bo.resource.docflow.connect=
jdbc\:vjdbc\:servlet\:http\://SERVER\:8080/DocflowWeb/vjdbc,__default__
```

4. В файлах **DocflowDesktop\install.cmd** и **DocflowDesktop\DocflowDesktop.cmd** в следующей строке заменить строку FLSSRV на сетевое имя файлового сервера:

```
SET SOURCE=\\FLSSRV\DocflowDesktop
```

Инсталляция клиентской части на рабочем компьютере пользователя.

Установка собственно клиентской части Системы должна выполняться на компьютере пользователя любым уполномоченным сотрудником. Все действия он должен выполнять как пользователь с административными полномочиями.

1. В каталоге **c:\Program Files** создать каталог **Zirvan\DoXLogic**, и дать права на модификацию его содержимого пользователям компьютера. Это необходимо для работы механизма автообновления клиентской части Системы.
2. С файлового ресурса **DocflowDesktop** запустить на выполнение командный файл **install.cmd**, который скопирует клиентскую часть desktop-приложения Системы на компьютер и создаст ярлыки для запуска на рабочем столе и в меню.

8. Инструкция по использованию КриптоПро в DoXLogic

8.1. Общие сведения об использовании КриптоПро в DoXLogic

В системе DoXLogic для работы с электронно-цифровой подписью (ЭЦП) можно использовать средства криптографической защиты информации (СКЗИ) КриптоПро CSP 3.6.

КриптоПро CSP 3.6 имеет сертификат соответствия ФСБ, на основании которого может использоваться для обеспечения целостности и подлинности информации, не содержащей сведений, составляющих государственную тайну. Поэтому КриптоПро целесообразно использовать вместо стандартных, встроенных в Windows, СКЗИ при организации юридически значимого документооборота на предприятиях.

Для хранения ключей в КриптоПро используются контейнеры, содержащие закрытый и открытый ключи. Контейнеры можно создавать на различных устройствах, в зависимости от установленных драйверов (TouchMemory, e-token, дискета, реестр Windows). Контейнеры могут быть защищены паролем, что обеспечивает двухуровневую аутентификацию и, как следствие, большую достоверность ЭЦП по сравнению с СКЗИ Windows.

8.2. Настройка использования КриптоПро в DoXLogic

7.2.1 Порядок настройки использования КриптоПро в DoXLogic

Чтобы начать использовать КриптоПро в DoXLogic, необходимо выполнить следующие действия:

- если Центр Сертификации не установлен, то установить его в соответствии с документом «Инструкция по установке и настройке Центра Сертификации»;
- установить и настроить ПО КриптоПро CSP на компьютерах администратора и пользователей, которые будут подписывать документы на основе сертификатов (пользователи СКЗИ);
- для этих пользователей сгенерировать ключевые пары и создать контейнеры;
- импортировать сертификаты в локальные хранилища сертификатов компьютера и зарегистрировать их в DoXLogic.

7.2.2 Установка ПО КриптоПро CSP на компьютеры с клиентской частью DoXLogic

Установка осуществляется при помощи пакета установки из поставки КриптоПро CSP (CSPrus.msi – русскоязычная версия, CSPeng.msi – англоязычная версия).

Установку можно проводить в скрытом режиме и в режиме с отображением пользовательского интерфейса.

Скрытый режим рекомендуется использовать при автоматической установке через Active Directory. В этом случае командная строка для установки русскоязычной версии CPRus.msi должна иметь следующий формат:

msiexec /i CSPrus.msi /qn

Режим с отображением пользовательского интерфейса рекомендуется использовать при ручной установке на компьютеры пользователя. В этом случае командная строка для установки русскоязычной версии должна выглядеть так:

msiexec /i CSPrus.msi /qb

7.2.3 Установка и настройка ПО КриптоПро CSP на компьютеры пользователей СКЗИ

Установка и настройка ПО КриптоПро CSP производится в соответствии с документом «Инструкция по использованию КриптоПро CSP и TLS» из поставки ПО КриптоПро CSP. Необходимо установить ПО и настроить считыватели (устройства), на которых будут храниться контейнеры.
Для всех носителей, определяемых Windows как сменные - гибких дисков, flash-дисков, ZIP - предназначен считыватель «дисковод».

Например, пользователь будет хранить контейнер на flash-диске. Windows при подключении диска присваивает ему букву F. В этом случае необходимо вставить flash-диск и в контрольной панели КриптоПро CSP добавить новый считыватель – дисковод F. Если пользователь имеет

несколько подобных устройств и возможна ситуация, когда при подключении будет присвоена буква, отличная от F, то необходимо добавить новый считыватель на каждую букву.

7.2.4 Генерация ключевой пары и создание контейнера

На компьютер, где будет осуществляться генерация ключевой пары, необходимо установить ПО КриптоПро CSP в соответствии с документом «Инструкция по использованию КриптоПро CSP и TLS».

Для генерации ключевой пары и создания контейнера, в котором она будет храниться, необходимо выполнить все шаги, описанные в руководстве администратора системы DoXLogic в разделе «Инструкция по работе с сертификатами в системе DoXLogic». Отличие: в выпадающем списке «CSP» необходимо выбрать один из криптопровайдеров КриптоПро (начинаются с «Crypto-Pro»). Будет предложено выбрать устройство для хранения контейнера и, если устройство имеет сменные носители, вставить носитель. Подробнее данная процедура описана в разделе «Интерфейс генерации ключей» инструкции по использованию КриптоПро CSP и TLS.

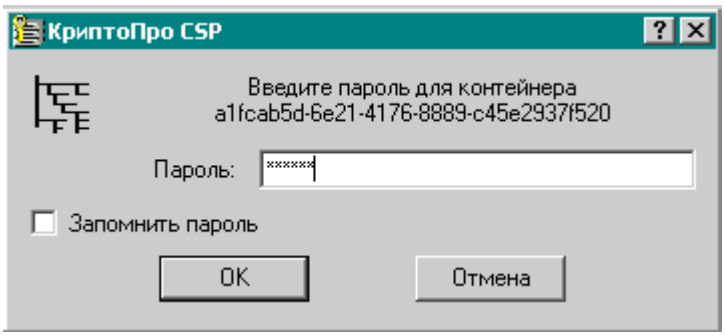
7.2.5 Импорт сертификатов в локальные хранилища и регистрация в DoXLogic

Чтобы использовать полученные ключи в DoXLogic, для каждого пользователя, имеющего контейнер, необходимо:

- импортировать сертификат из контейнера в локальное хранилище сертификатов компьютера. Для этого необходимо проделать шаги, описанные в разделе «Просмотр и установка личного сертификата, хранящегося в контейнере закрытого ключа» инструкции по использованию КриптоПро CSP и TLS;

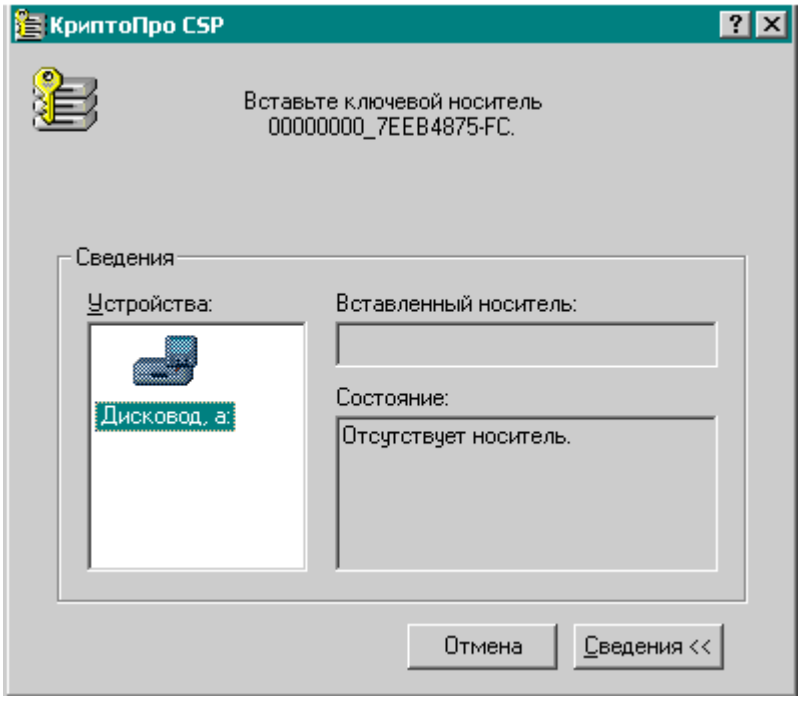
8.3. Установка ЭЦП и подписание документа сертификатом из контейнера

Чтобы подписать документ электронной цифровой подписью (ЭЦП) на основе сертификата, необходимо проделать те же действия, что и при использовании обычного сертификата (см. руководство пользователя системы DoXLogic). Отличия заключаются в дополнительных диалоговых окнах. Так, при попытке подписания документа сертификатом из контейнера, на котором установлен пароль, будет выведено окно запроса пароля.



Галочка «Запомнить пароль» позволяет избежать повторного ввода пароля в течение текущего сеанса пользователя (до выхода пользователя из Windows).

После ввода пароля, если носитель с контейнером не вставлен, то будет предложено выбрать устройство и вставить носитель.



Устройства, зарегистрированные в КриптоПро, могут быть различны. Все сменные носители (flash-drive, дискеты, ZIP) в списке устройств будут именоваться как «Дисковод», с указанием соответствующей буквы диска. В случае, если носитель с контейнером вставлен, но Windows присвоила ему букву диска, которой нет в списке устройств, необходимо либо переопределить букву диска средствами оснастки Windows «Управление дисками», либо зарегистрировать новый дисковод с данной буквой диска при помощи контрольной панели КриптоПро CSP (см. инструкцию по использованию КриптоПро CSP и TLS).

9. Инструкция по настройке полнотекстового поиска по содержимому файлов документов

9.1. Настройка полнотекстового поиска по содержимому текстовых pdf-файлов для sql server (64 бит)

1. Проинсталлировать фильтр **PDFiFilter64installer.msi** из дистрибутива на сервер БД.
2. Добавить путь к подкаталогу bin каталога, в который проинсталлирован фильтр в переменную среды PATH.

   C:\Program Files\Adobe\Adobe PDF iFilter 9 for 64-bit platforms\bin

3. Выполнить на sql server скрипт.

```
exec sp_fulltext_service 'load_os_resources', 1
exec sp_fulltext_service 'verify_signature', 0
go
```

4. Перезапустить sql server (службы ***SQL Server (MS SQL SERVER)*** и ***SQL Full-text Filter Daemon Launcher (MSSQL SEREVER)***).
5. Выполнить на sql server скрипт.

```
exec sp_fulltext_service 'update_languages'
exec sp_fulltext_service 'restart_all_fdhosts'
go
```

6. Убедиться, что фильтр проинсталлировался, выполнив на sql server команду:

   select document_type, path from sys.fulltext_document_types where document_type = '.pdf'

7. Перезаполнить каталог, выполнив на sql server скрипт:

```
ALTER FULLTEXT CATALOG zirvan_search_catalog REBUILD;
go
```

Примечание.

Данный этап настройки может занять значительное время.

9.2. Настройка полнотекстового поиска по содержимому файлов пакета Office2007 для sql server (64 бит)

1. Проинсталлировать фильтр **FilterPack64bit.exe** из дистрибутива на сервер БД.
2. Добавить путь к каталогу, в который проинсталлирован фильтр в переменную среды PATH.

   C:\Program Files\Common Files\Microsoft Shared\Filters

3. Выполнить на sql server скрипт.

```
exec sp_fulltext_service 'load_os_resources', 1
exec sp_fulltext_service 'verify_signature', 0
go
```

4. Перезапустить sql server (службы ***SQL Server (MS SQL SERVER)*** и ***SQL Full-text Filter Daemon Launcher (MSSQL SEREVER)***).
5. Выполнить на sql server скрипт.

```
exec sp_fulltext_service 'update_languages'
exec sp_fulltext_service 'restart_all_fdhosts'
go
```

6. Убедиться, что фильтр проинсталлировался, выполнив на sql server команду:

```
select document_type, path from sys.fulltext_document_types where document_type = '.docx'
```

7. Перезаполнить каталог, выполнив на sql server скрипт:

```
ALTER FULLTEXT CATALOG zirvan_search_catalog REBUILD;
go
```

Примечание.

Данный этап настройки может занять значительное время.

При одновременной настройке полнотекстового поиска по содержимому pdf-файлов и содержимому файлов пакета Office2007 настройку можно выполнить в следующем порядке:

1. Шаги 1 и 2 из п. 9.1 **и** п. 9.2 настоящего руководства;
2. Шаги 3, 4 и 5 из п. 9.1 **или** п. 9.2 настоящего руководства;
3. Шаги 6 из п. 9.1 **и** п. 9.2 настоящего руководства;
4. Шаг 7 из п. 9.1 **или** п. 9.2 настоящего руководства.

10. Первичная проверка корректности установки СЭД «DoXLogic»

Для первичной проверки корректности установки всех компонент СЭД необходимо последовательно выполнить следующие действия:

1. Подключиться к БД СЭД через Desktop приложение под учетной записью admin (пароль admin).
2. Убедиться в успешности подключения к БД СЭД сервиса jScheduler.Server (см.п. 4.4).
3. Подключиться к БД СЭД через Web приложение под учетной записью admin (пароль admin).