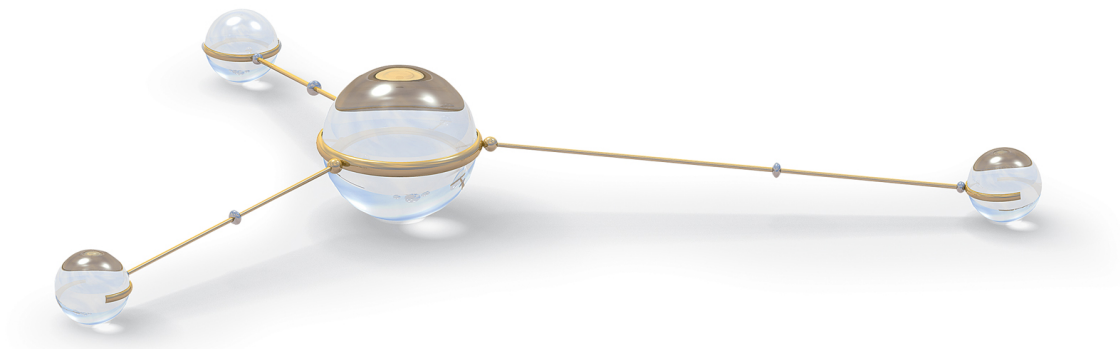




## Система "ДБО BS-Client"

Релиз 017.7.200, Централизованная схема  
Документация клиента "Интернет-Клиент"

# **Руководство по установке, настройке и обновлению АРМ клиента подсистемы *Интернет- Клиент***



Система "ДБО BS-Client"

Релиз 017.7.200, Централизованная схема

## Документация клиента "Интернет-Клиент"

Руководство по установке, настройке и обновлению АРМ клиента подсистемы *Интернет-Клиент*

**Опубликовано 2010**

Листов 32

© 2010 ООО "БСС"

Настоящий документ содержит информацию, актуальную на момент его составления. ООО "БСС" не гарантирует отсутствия ошибок в данном документе. ООО "БСС" оставляет за собой право вносить изменения в документ без предварительного уведомления.

Никакая часть данного документа не может быть воспроизведена или передана в какой бы то ни было форме и какими бы то ни было средствами без письменного разрешения ООО "БСС".

ООО "БСС" не гарантирует, что специфицированное в настоящем документе программное обеспечение не содержит дефектов, будет работать в произвольно выбранных условиях и при этом удовлетворять всем требованиям, которые могут быть к нему предъявлены.

ООО "БСС" не гарантирует работоспособность нелегально полученного программного обеспечения. Нелегальное использование программного обеспечения и документации на него преследуется законом.

Наименование ООО "БСС", товарный знак , продукты и их наименования "Система Дистанционного Банковского Обслуживания BS-Client" ("ДБО BS-Client") являются интеллектуальной собственностью ООО "БСС" и охраняются действующим законодательством.

Все иные упомянутые в настоящем документе марки, названия продуктов и фирм могут являться интеллектуальной собственностью соответствующих владельцев.

© 2010 ООО "БСС"

## Содержание

Введение .....	4
Глоссарий .....	6
1. Общие сведения .....	7
1.1. Обеспечение безопасности данных .....	7
1.1.1. Защита ключей .....	7
1.2. Требования к стороннему ПО .....	7
1.3. Описание процесса подготовки АРМ клиента подсистемы <i>Интернет-Клиент</i> .....	8
1.4. Описание процесса обновления компонентов АРМ клиента .....	9
1.5. Особенности использования браузеров и ОС различных версий .....	9
1.5.1. Особенности загрузки страниц в Internet Explorer 6.0 (разрешенные сайты) .....	9
1.5.2. Особенности работы с ОС Windows Vista .....	10
1.5.3. Особенности печати документов в Internet Explorer .....	11
1.5.4. Особенности масштабирования в Internet Explorer .....	12
2. Инструкции по подготовке АРМ .....	13
2.1. Настройка сопутствующего ПО .....	13
2.1.1. Настройка браузера Internet Explorer .....	13
2.1.2. Настройка Windows Vista .....	20
2.2. Установка / обновление компонентов АРМ клиента подсистемы <i>Интернет-Клиент</i> .....	23
2.3. Начальная настройка подсистемы <i>Интернет-Клиент</i> .....	25
2.3.1. Начальная настройка параметров входа в систему с типом защиты канала односторонний SSL .....	26
А. Параметры СКЗИ, доступные для редактирования .....	29
А.1. Excellence 4.0 .....	29
А.2. Crypto-C .....	29
А.3. Crypto COM/2.2 .....	29
А.4. OpenSSL .....	29
А.5. Verba-OW/4 .....	30
А.6. CryptoPro CSP/1.1 .....	30
А.7. Ms Crypto API 2.0 .....	30
А.8. LAN Crypto/2.35 .....	31
А.9. Message-PRO 1.1, 1.3x, 2.x, 3.x .....	31
А.10. Крипто-КОМ 3.2 .....	31
А.11. Агава-С .....	32

# Введение

Настоящий документ является частью документации по системе "ДБО BS-Client" релиза 017.7.200, функционирующей в режиме Централизованной схемы.

## На кого ориентирован документ

Документ предназначен для

## Назначение документа

Назначение документа состоит в предоставлении информации об установке, настройке и обновлении АРМ клиента подсистемы *Интернет-Клиент*.

## Организация документа

В гл. 1 «Общие сведения» [стр. 7] приводится общая информация о подсистеме *Интернет-Клиент*.

В гл. 2 «Инструкции по подготовке АРМ» [стр. 13] приведены подробные инструкции по установке, настройке и обновлении АРМ клиента подсистемы *Интернет-Клиент*.

## Рекомендации по использованию документа

Документ рекомендуется использовать и в качестве ознакомительного материала, и в качестве справочника при работе с системой "ДБО BS-Client". Документ рекомендован как для последовательного, так и для выборочного изучения.

### Внимание!

Для интенсивного изучения документации и быстрого поиска необходимой информации рекомендуется воспользоваться контекстной справкой системы "ДБО BS-Client".

## Соглашения по оформлению

Кавычками выделяются значения полей экранных форм и различных параметров.

Наименования разделов и пунктов меню отделяются друг от друга символом →.

Для выделения блоков текста используются специальные средства оформления, представленные ниже.

### Примечание

Служит для выделения дополнительной или разъясняющей информации, в том числе ссылок на фрагменты документации, содержащие более подробные сведения. В основном следует непосредственно за элементом, к которому оно относится, но может предшествовать целой главе или разделу.

**Внимание!**

Служит для выделения важной информации, на которую следует обратить внимание.

Служит для выделения дополнительной информации, рекомендованной для углубленного изучения системы. В основном информация, помеченная подобным образом, представляет собой описание редко используемых возможностей системы. Данную информацию можно пропустить при ознакомительном чтении.

# Глоссарий

## Перечень сокращений

АРМ	<i>Автоматизированное рабочее место.</i>
ДБО	Дистанционное банковское обслуживание. См. также Централизованная система "ДБО BS-Client".
ОС	Операционная система.
ОСПО	Окружающее и сопутствующее программное обеспечение.
ПО	Программное обеспечение.
РМ	<i>Рабочее место.</i>
ЦС "ДБО BS-Client"	<i>Централизованная система "ДБО BS-Client".</i>

## Перечень терминов

Автоматизированное рабочее место	<p>Автоматизированное рабочее место (<i>АРМ</i>) - совокупность компонентов системы "ДБО BS-Client". АРМ бывают трех видов:</p> <ul style="list-style-type: none"><li>• <i>АРМ банка</i> - совокупность компонентов системы, установленных на всех рабочих станциях и серверах <i>головного подразделения</i> и всех <i>подразделений</i> банка, имеющих непосредственный доступ к БД банка;</li><li>• <i>АРМ удаленной площадки</i> - совокупность компонентов системы, установленных в удаленной площадке подразделения банка, не имеющей непосредственного доступа к БД банка и осуществляющей взаимодействие с АРМ банка посредством подсистемы "Оператор Штрих-Кодов";</li><li>• <i>АРМ клиента</i> - совокупность компонентов системы, установленных на всех рабочих станциях клиента.</li></ul>
Инструкция	<p>В рамках документации по системе "ДБО BS-Client" – подробное описание последовательности действий, которые необходимо выполнить в системе "ДБО BS-Client" или в сторонней системе для решения некоторой элементарной задачи: осуществления операции над одним или несколькими объектами системы, запуска приложения, задания значений конфигурационных параметров и т.д. Примеры инструкций: создание / редактирование <i>документа ДБО</i>, подпись <i>документа ДБО</i>, изменение пароля для входа в систему. Порядок выполнения инструкций определяется регламентами по работе с системой.</p>
Клиент	Юридическое лицо, обслуживаемое системой.

# Глава 1. Общие сведения

## 1.1. Обеспечение безопасности данных

Подсистема *Интернет-Клиент* обеспечивает безопасность и конфиденциальность документооборота с банком за счет использования различных систем криптографической защиты информации, в том числе сертифицированных ФСБ. При работе с системой *Интернет-Клиент* весь трафик проходит через механизмы обеспечения безопасности соединения с банком – протоколы SSL или TLS, позволяющие повысить надежность связи и достичь юридически значимого документооборота. Подсистема *Интернет-Клиент* обеспечивает клиенту банка универсальность средств доступа к сети Интернет (при этом доступ к системе может быть осуществлен из любой точки мира с любого компьютера – достаточно иметь дискету с ключами электронно-цифровой подписи – ЭЦП) и возможность распределенного доступа к документам лиц, имеющих право первой, второй подписи, что позволяет им утверждать платежный документ без обязательного одновременного присутствия в конкретном месте.

### 1.1.1. Защита ключей

Так как подсистема *Интернет-Клиент* предназначена для работы с финансовыми документами, то пользователю стоит уделять повышенное внимание вопросам безопасности. Механизмом идентификации и основным механизмом защиты данных в подсистеме является ключ СКЗИ, хранящийся на сменном носителе, поэтому необходимо исключить доступ к сменному носителю посторонних лиц. Сменный носитель необходимо:

- хранить в недоступном месте;
- не оставлять в компьютере.

Также не стоит копировать ключи, хранящиеся на сменном носителе, на жёсткий диск компьютера.

Для уменьшения обращений к ключевой дискете после входа в подсистему ключевая информация загружается в память компьютера и остается доступной без обращений к ключевой дискете в течение всей работы. Ключевая информация удаляется из памяти через 5 минут после последнего к ней обращения, либо при выходе из подсистемы. Поэтому, после завершения работы необходимо обязательно выйти из подсистемы.

## 1.2. Требования к стороннему ПО

Стороннее программное обеспечение должно быть установлено до установки компонентов АРМ клиента подсистемы *Интернет-Клиент*. Требования к стороннему программному обеспечению приведены в следующей таблице.

Таблица 1.1. Требования к стороннему ПО АРМ клиента подсистемы *Интернет- Клиент*

Вид ПО	Наименование ПО	Версии ПО		Примечания
		Рекоменд.	Поддерж.	
ОС	Windows	XP, 2003	2000, Vista, 2008, Windows 7 (Ultimate, Professional, Enterprise, Home Premium, Home Basic)	Для работы с ОС Windows Vista требуется специальная настройка ОС. Windows Vista и Windows 7 поддерживаются только в реализации x86
Веб-браузер	Microsoft Internet Explorer	8.0	6.0, 7.0	
Текстовый процессор	Microsoft Word	XP, 2003		Не обязательно. Для чтения RTF-файлов документов, сформированных с помощью подсистемы
	OpenOffice		2.3.0, 3.x	
ПО для работы с документацией	Adobe Reader, Adobe Acrobat Standart, Adobe Acrobat Professional	5.0 и выше	5.0 и выше	Необходимо для чтения документации подсистемы

### 1.3. Описание процесса подготовки АРМ клиента подсистемы *Интернет-Клиент*

**Внимание!**

Пользователю, проводящему установку СПО, необходимо иметь права локального администратора ОС.

Перед эксплуатацией подсистемы *Интернет-Клиент* необходимо осуществить установку и настройку компонентов подсистемы в следующем порядке:

1. Настройка сопутствующего программного обеспечения, необходимого для нормальной работы с подсистемой.
  - a. Перечень стороннего программного обеспечения, которое необходимо предварительно установить на АРМ клиента, приведен в разд. 1.2 «Требования к стороннему ПО» [стр. 7]. При выборе версий стороннего ПО необходимо руководствоваться особенностями использования ПО (см. разд. 1.5 «Особенности использования браузеров и ОС различных версий» [стр. 9]).
  - b. В случае соединения с банком по протоколу TLS необходимо предварительно выполнить установку сертификата, выданного банком на АРМ пользователя подсистемы. Для установки сертификата воспользуйтесь документацией разработчика.

- с. Для настройки СПО выполните действия, описанные в гр. инстр. «Настройка сопутствующего ПО» [стр. 13].
2. Установка компонентов подсистемы *Интернет-Клиент* на АРМ клиента. Для установки компонентов (cab-файлов) выполните действия, описанные в инстр. «Установка / обновление компонентов АРМ клиента подсистемы Интернет-Клиент» [стр. 23].
3. Настройка параметров входа в систему с типом защиты канала односторонний SSL. Для настройки параметров входа выполните действия, описанные в инстр. «Начальная настройка параметров входа в систему с типом защиты канала односторонний SSL» [стр. 26].

## 1.4. Описание процесса обновления компонентов АРМ клиента

Обновление компонентов АРМ клиента подсистемы *Интернет-Клиент* инициируется на стороне банка. Если на сервере банка появился пакет обновлений (cab-файлы) АРМ, то при входе на главную страницу сайта или после входа в подсистему будет предложено установить компоненты ActiveX. Для того чтобы установить компоненты АРМ клиента подсистемы выполните действия, описанные в инстр. «Установка / обновление компонентов АРМ клиента подсистемы Интернет-Клиент» [стр. 23].

### Примечание

Порядок действий, который необходимо выполнить для установки пакета обновлений не отличается от порядка действий при первоначальной установке компонентов подсистемы, производимый с сайта банка.

В случае отказа от установки пакета обновлений нет гарантии, что подсистема будет работать должным образом.

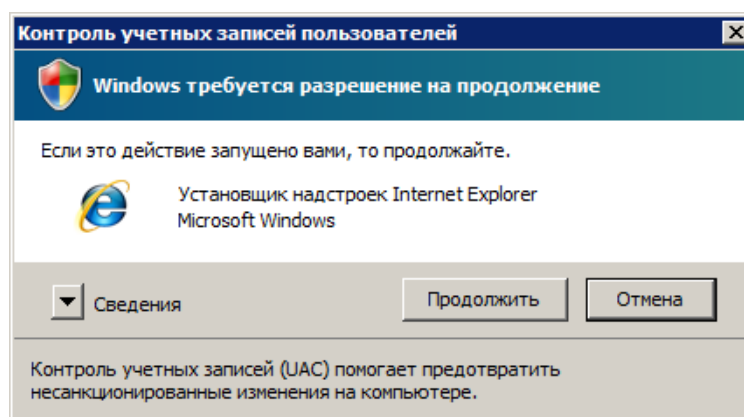
## 1.5. Особенности использования браузеров и ОС различных версий

### 1.5.1. Особенности загрузки страниц в Internet Explorer 6.0 (разрешенные сайты)

При использовании браузера Internet Explorer 6.0 с типом защиты канала SSL и использовании обозревателем политики безопасности "разрешенные сайты" в процессе работы с подсистемой на экране периодически появляется сообщение о наличии небезопасных элементов. Периодическое появление сообщения затрудняет работу пользователя с подсистемой, так как требуется постоянное подтверждение загрузки небезопасных элементов. Для того чтобы устранить появление сообщений при работе с подсистемой необходимо отключить политику "разрешенные сайты". Описание действий, необходимых для отключения политики "разрешенные сайты", содержатся в инструкции по настройке браузера Internet Explorer (см. инстр. «Настройка браузера Internet Explorer» [стр. 13]). Если отключение политики "разрешенные сайты" неприемлемо, то рекомендуется установить другую версию браузера.

## 1.5.2. Особенности работы с ОС Windows Vista

В ОС Windows Vista реализован механизм контроля учетных записей пользователей (UAC), призванный повысить безопасность системы. Данный механизм в числе прочего осуществляет контроль обращения приложений к файлам жесткого диска. При попытках записи приложением данных на жесткий диск, а также при попытках установки программного обеспечения, механизм контроля учетных записей либо требует подтверждения необходимости выполнения действия (см. рис. 1.1), либо запрещает его.



**Рис. 1.1.** Запрос UAC подтверждения необходимости выполнения действия

Поскольку клиентская часть подсистемы *Интернет-Клиент* в процессе своей работы обращается к файлам жесткого диска, то для полноценной работы требуется либо постоянное подтверждение необходимости выполнения действия, либо отключение контроля учетных записей.

Обращение клиентской части подсистемы *Интернет-Клиент* к жесткому диску осуществляется в следующих случаях:

- Установка загружаемых при входе на сайт cab-файлов криптографических библиотек и компонентов ActiveX. В процессе установки UAC будет запрашивать подтверждения о необходимости проведения установки (см. рис. 1.1).
- Осуществление криптографических операций подписи документов и проверки подписи. Если криптографические ключи хранятся на жестком диске компьютера, то при использовании ряда криптографий UAC запрещает обращение к криптографическим ключам (см. рис. 1.2). В этом случае необходимо либо размещение криптографических ключей на сменных носителях (см. разд. 8.4 «Настройка параметров ключевых носителей абонентов ЭЦП» док. *Руководство пользователя*), либо отключение UAC (см. инстр. «Настройка Windows Vista» [стр. 20]).

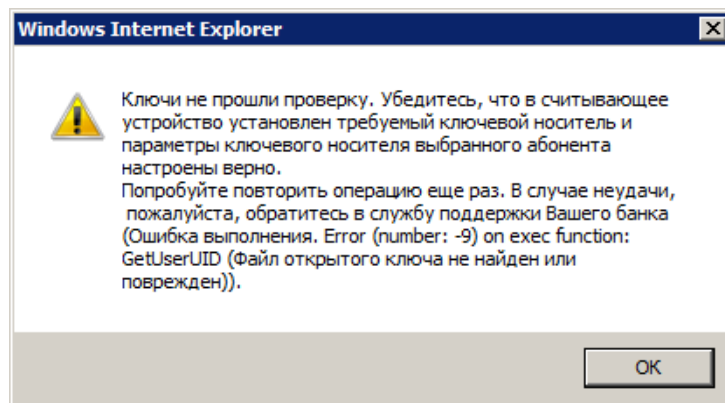


Рис. 1.2. Сообщение, возникающее при запрете УАС обращения к криптографическим ключам

- Сохранение параметров ключевых носителей локально в файле на жестком диске (см. разд. 8.4 «Настройка параметров ключевых носителей абонентов ЭЦП» док. *Руководство пользователя*). При попытках сохранения параметров на жестком диске УАС запрещает обращение к диску. В этом случае также необходимо либо размещение файла с параметрами ключевых носителей на сменных носителях, либо отключение УАС (см. инстр. «Настройка Windows Vista» [стр. 20]).

Остальные процессы, выполняемые клиентской частью подсистемы *Интернет-Клиент*, при использовании Windows Vista протекают так же, как при использовании более ранних продуктов семейства Windows.

Для отключения контроля учетных записей, если это необходимо, выполните действия, описанные в инстр. «Настройка Windows Vista» [стр. 20].

### 1.5.3. Особенности печати документов в Internet Explorer

Печать документов в браузере Internet Explorer может осуществляться некорректно в случае использования для параметров печати значений по умолчанию или недопустимых значений: печатаемая форма может не полностью помещаться на лист. Для корректной печати документов необходимо изменить значения параметров печати браузера Internet Explorer в соответствии с п. 12 - п. 19 инстр. «Настройка браузера Internet Explorer» [стр. 13].

#### Примечание

При использовании браузера Internet Explorer 7.0 может возникать проблема, связанная с невозможностью запрета автоматического сжатия печатаемых форм до размеров страницы. Автоматическое сжатие при некорректно заданных размерах полей страницы может приводить к недопустимой степени сжатия печатаемых форм. В случае если в Вашей версии браузера отсутствует возможность управления автоматическим сжатием при печати, установите последний пакет обновления для ОС Windows. Подробная информация об описанной проблеме изложена в следующей статье: <http://support.microsoft.com/kb/932538/>.

#### 1.5.4. Особенности масштабирования в Internet Explorer

При работе с некоторыми видами документов в браузере Internet Explorer отдельные из полей могут отображаться некорректно. Это может быть связано с неправильным выбором масштаба веб-страницы. Для корректного отображения всех полей в документах необходимо перед началом работы в браузере Internet Explorer установить масштаб "100%".

## Глава 2. Инструкции по подготовке АРМ

### 2.1. Настройка сопутствующего ПО

Настройку сопутствующего ПО необходимо выполнить для подготовки АРМ клиента подсистемы *Интернет-Клиент* (см. разд. 1.3 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 8]).

#### 2.1.1. Настройка браузера Internet Explorer

Для настройки браузера Internet Explorer:

1. Стандартным образом откройте обозреватель Internet Explorer.
2. В зависимости от версии браузера выполните команду меню:
  - a. для Internet Explorer 6.0 выполните **Сервис (Tools) → Свойства обозревателя (Internet Options)**;
  - b. для Internet Explorer 7.0 выполните **Сервис (Tools) → Свойства обозревателя (Internet Options)**.
  - c. для Internet Explorer 8.0 выполните **Сервис (Tools) → Свойства обозревателя (Internet Options)**.
3. Откроется окно **Свойства Обозревателя (Internet Options)**.
4. Перейдите на закладку **Безопасность (Security)**.

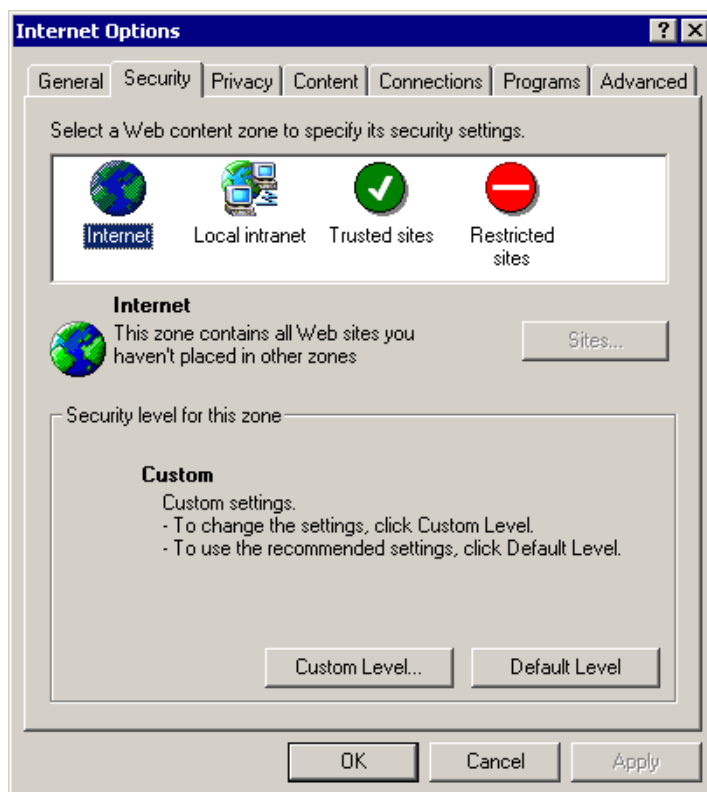


Рис. 2.1. Закладка Безопасность окна Свойства обозревателя браузера Internet Explorer 6.0

## Инструкции по подготовке АРМ

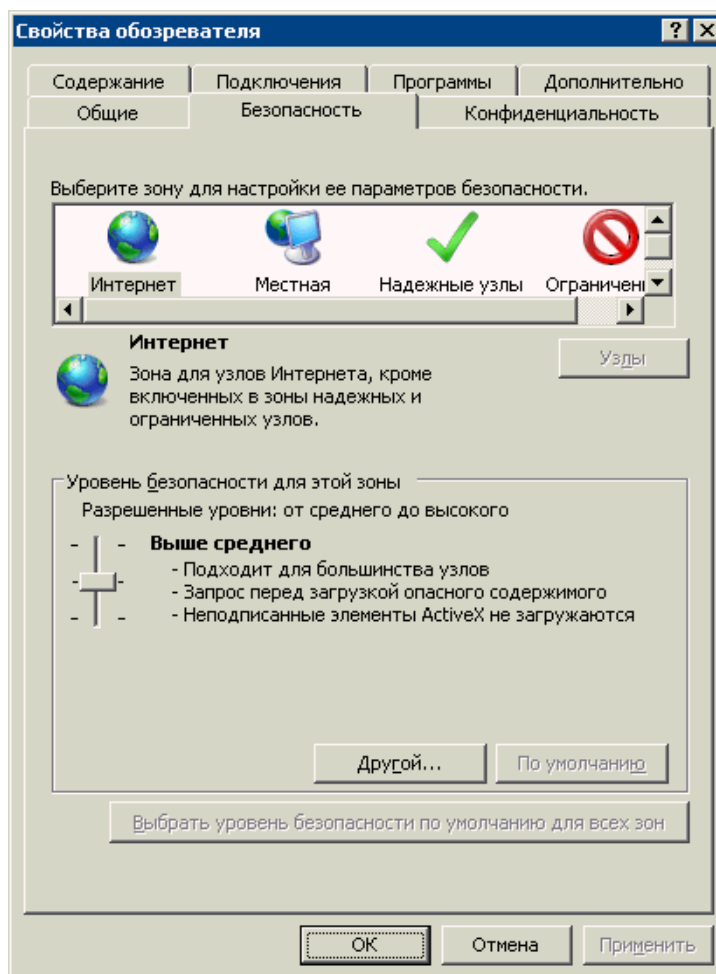


Рис. 2.2. Закладка безопасность окна Свойства обозревателя браузера Internet Explorer 7.0

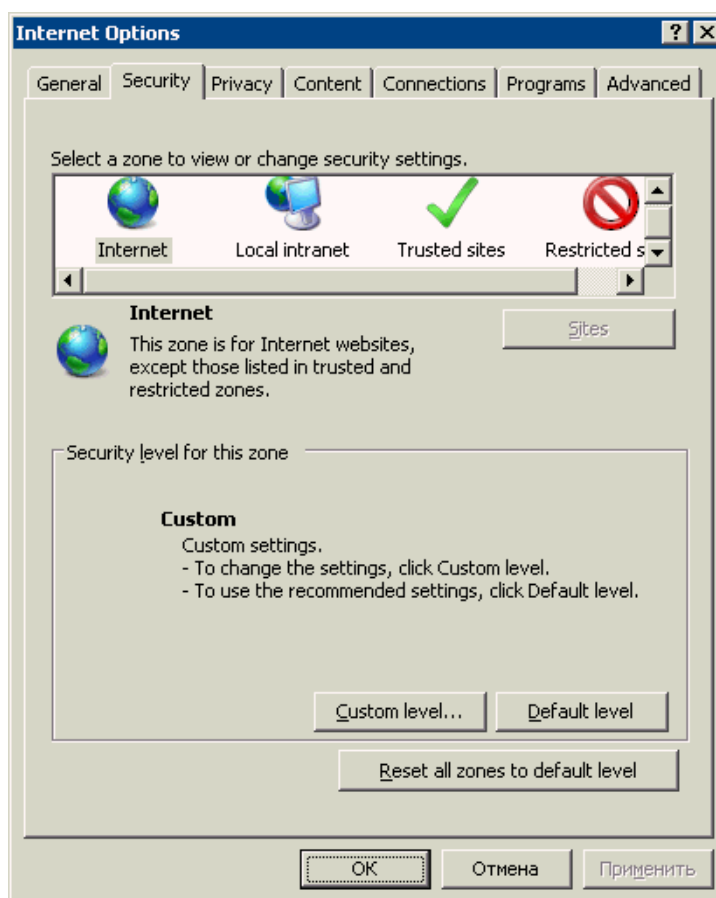
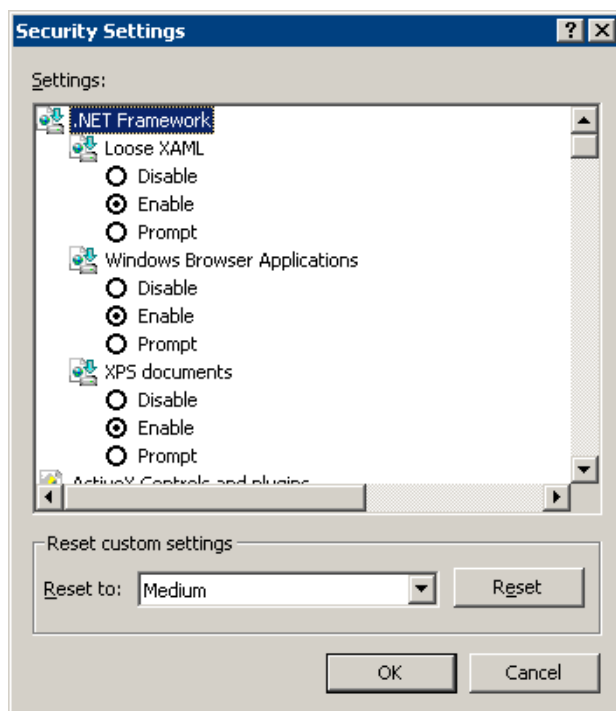


Рис. 2.3. Закладка безопасность окна Свойства обозревателя браузера Internet Explorer 8.0

5. Выберите зону "Интернет" ("Internet") для настройки её безопасности .
6. В блоке **Уровень безопасности для этой зоны (Security level for this zone)** нажмите последовательно кнопку **По умолчанию (Default level)** затем кнопку **Другой... (Custom level...)**.
7. Откроется окно **Правила безопасности (Security level)**.



**Рис. 2.4. Окно Правила безопасности**

8. В блоке **Параметры (Settings)** заполните поля параметров согласно значениям, приведённым в следующей таблице.

**Примечание**

Английские и русские термины приведены через косую черту.

**Таблица 2.1. Параметры безопасности для браузера Internet Explorer**

Настройка	Значение	Примечание
ActiveX controls and plug-ins / Элементы ActiveX и модули подключения		
Download signed ActiveX controls / Загрузка подписанных элементов ActiveX	Enable / Разрешить	
Download unsigned ActiveX controls / Загрузка неподписанных элементов ActiveX	Disable / Отключить	
Initialize and script ActiveX controls not marked as safe / Использование элементов ActiveX, не помеченных как безопасные	Disable / Отключить	
Run ActiveX controls and plug-ins / Запуск элементов ActiveX и модулей подключения	Enable / Разрешить	
Script ActiveX controls marked safe for scripting / Выполнять сценарии элементов ActiveX, помеченных как безопасные	Enable / Разрешить	
Automatic prompting for ActiveX controls / Автоматические запросы элементов управления ActiveX	Enable / Разрешить	

## Инструкции по подготовке АРМ

Cookies / Файлы "cookie"		
Allow cookies that are stored on your computer / Разрешить использование файлов «cookie», которые хранятся на вашем компьютере	Enable / Разрешить	
Allow per-session cookies (not stored) / Разрешить использовать во время сеанса файлов «cookie» (из сети)	Enable / Разрешить	
Downloads / Загрузка		
File download / Загрузка файла	Enable / Разрешить	
Font download / Загрузка шрифта	Prompt / Предлагать	
Java / Язык Java		
Java permissions / Разрешения Java	High safety / Высокая безопасность	
Miscellaneous / Разное		
Access data sources across domains / Доступ к источникам данных за пределами домена	Disable / Отключить	
Drag and drop or copy and paste files / Перетаскивание или копирование и вставка файлов	Prompt / Предлагать	
Installation of desktop items / Установка элементов рабочего стола	Disable / Отключить	
Launching programs and files in an IFRAME / Запуск приложений и файлов в окне IFRAME	Disable/Отключить	
Navigate sub-frames across different domains / Переход между кадрами через разные домены	Disable / Отключить	
Software channel permissions / Разрешения канала программного обеспечения	High safety / Высокая безопасность	
Submit nonencrypted form data / Передача незашифрованных данных форм	Enable / Разрешить	
Userdata persistence / Устойчивость данных пользователя	Enable / Разрешить	
Allow script-initiated windows without size or position constraints / Разрешать запущенные сценарием окна без ограничений на размеры и положение	Enable / Разрешить	Необходимо настроить параметр для браузеров версии 6.0 и выше
Scripting / Сценарии		
Active scripting / Активные сценарии	Enable / Разрешить	
Allow paste operations via script / Разрешить операции вставки из сценария	Disable / Отключить	
Scripting of Java applets / Выполнять сценарии приложений Java	Disable / Отключить	

9. Нажмите кнопку **ОК** окна **Правила безопасности (Security level)** для завершения настройки параметров безопасности.

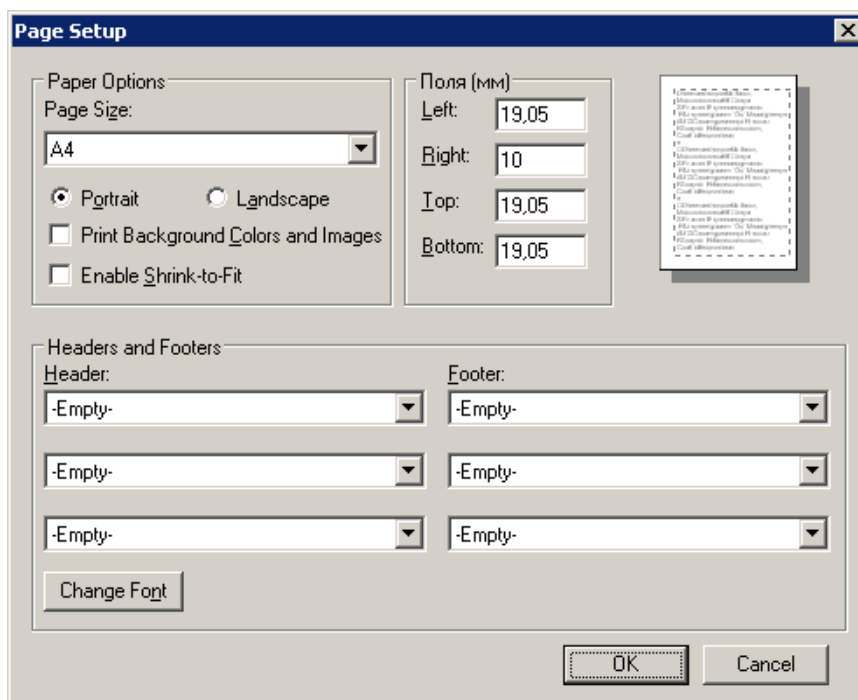
## Инструкции по подготовке АРМ

10. Для браузера Internet Explorer 6.0 отключите политику безопасности "разрешенные сайты", если это необходимо (см. разд. 1.5.1 «Особенности загрузки страниц в Internet Explorer 6.0 (разрешенные сайты)» [стр. 9]):
  - a. Перейдите на закладку **Содержание (Content)** окна **Свойства Обозревателя (Internet Options)**.
  - b. В блоке **Разрешенные сайты (Content Advisor)** нажмите кнопку **(Disable)**.

**Примечание**

Если политика безопасности отключена, т.е. в блоке **Ограничение доступа (Content Advisor)** отображена кнопка **Включить (Enable)**, то перейдите к следующему шагу инструкции.

11. Нажмите последовательно кнопку **Применить (Apply)**, затем кнопку **ОК** для сохранения сделанных изменений.
12. Выполните команду меню **Файл (File) → Параметры страницы (Page Setup)**.
13. Откроется окно **Параметры страницы (Page Setup)**.



**Рис. 2.5. Окно Параметры страницы (Page Setup)**

14. В блоке **Параметры бумаги (Paper Options)** заполните поле выбора **Книжная (Portrait)**.
15. Для полей блока **Поля (мм) (Margins (millimeters))** установите следующие значения:
  - a. **Левое (Left)** – не более "19,05";

- b. **Правое (Right)** – не более "10";
  - c. **Верхнее (Top)** – не более "19,05";
  - d. **Нижнее (Bottom)** – не более "19,05".
16. Во всех полях выбора блока **Колонтитулы (Headers and Footers)** выберите значение "-Пусто-" (" -Empty- ").
17. В некоторых версиях браузера Internet Explorer реализована возможность уменьшения размеров печатаемого документа до размеров страницы. В случае если необходимо активировать автоматическое сжатие при печати, заполните поле **Сжимать по размеру страницы (Enable Shrink-toFit)**.

**Примечание**

При использовании некоторых версий браузера Internet Explorer функция автоматического сжатия при печати может быть включена без возможности ее отключения. Решение проблемы управления автоматическим сжатием описано в разд. 1.5.3 «Особенности печати документов в Internet Explorer» [стр. 11].

18. Для остальных параметров оставьте значения по умолчанию.
19. Нажмите кнопку **ОК** для сохранения выполненных изменений.

## 2.1.2. Настройка Windows Vista

В случае использования ОС Windows Vista рекомендуется отключить механизм контроля учетных записей (см. разд. 1.5.2 «Особенности работы с ОС Windows Vista» [стр. 10]).

Отключение механизма контроля учётных записей, если это необходимо, осуществляется следующим образом:

1. Отобразите панель управления Windows (Control Panel).

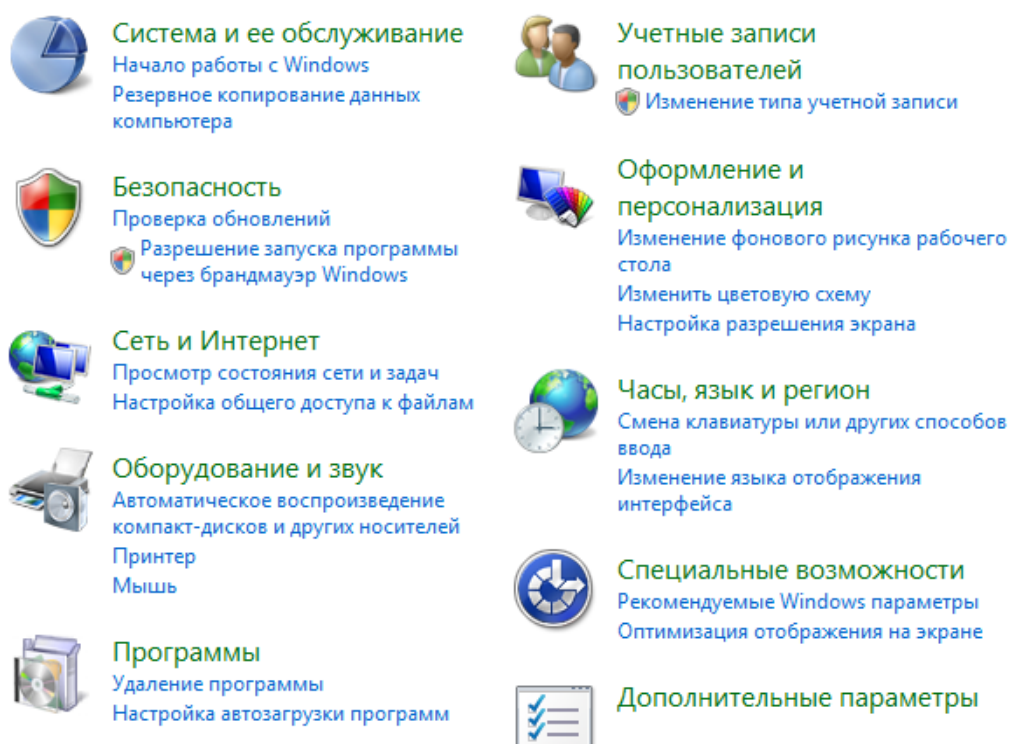


Рис. 2.6. Фрагмент панели управления Windows

2. Выберите пункт **Учетные записи пользователей**.
3. Система отобразит окно настройки учетных записей пользователей.

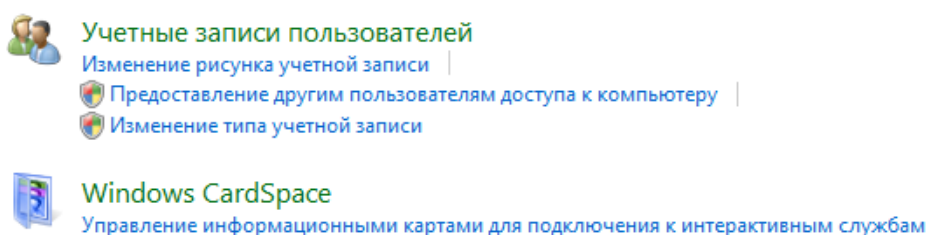
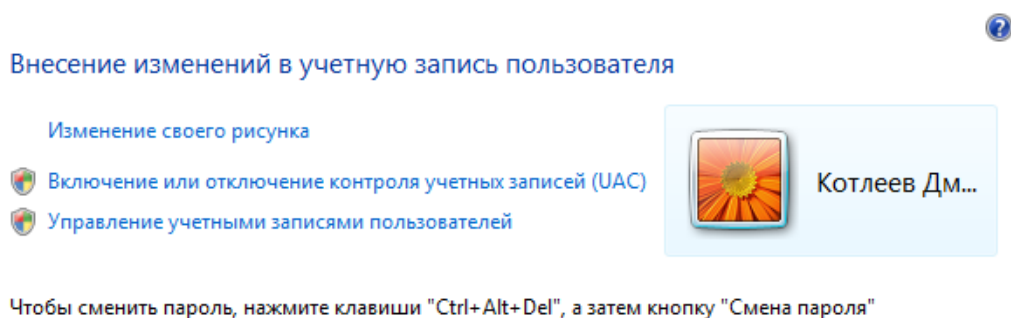


Рис. 2.7. Окно настройки учетных записей пользователей

4. Выберите пункт **Учетные записи пользователей**.
5. Система отобразит окно изменения параметров учетной записи пользователя.



**Рис. 2.8. Окно изменения параметров учетной записи пользователя**

6. Выберите пункт **Включение или отключение контроля учетных записей (UAC)**.
7. Система отобразит сообщение UAC о необходимости подтверждения действия.
8. Нажмите кнопку **Продолжить**.
9. Система отобразит окно изменения параметров UAC.

#### Включить контроль учетных записей (UAC) для повышения безопасности

Контроль учетных записей (UAC) помогает предотвратить несанкционированные изменения на компьютере. Рекомендуется не отключать контроль учетных записей, что повышает защищенность компьютера.

Используйте контроль учетных записей (UAC) для защиты компьютера



**Рис. 2.9. Окно изменения параметров UAC**

10. Снимите заполнение поля **Используйте контроль учетных записей (UAC) для защиты компьютера**.
11. Нажмите кнопку **ОК**.
12. Система выведет предложение произвести перезагрузки системы.
13. Нажмите кнопку **Перезагрузить сейчас**.
14. Система осуществит перезагрузку системы.

После выполнения указанных действий контроль учетных записей пользователей будет отключен.

## 2.2. Установка / обновление компонентов АРМ клиента подсистемы *Интернет-Клиент*

Установку компонентов АРМ клиента подсистемы необходимо осуществлять после настройки сопутствующего ПО (см. разд. 1.3 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 8]).

Обновление компонентов АРМ клиента подсистемы может осуществляться только с сайта банка (см. разд. 1.4 «Описание процесса обновления компонентов АРМ клиента» [стр. 9]).

Для установки / обновления компонентов подсистемы *Интернет-Клиент* выполните следующие действия:

1. Запустите мастер установки компонентов АРМ подсистемы *Интернет-Клиент* с сайта банка либо из дистрибутива.
  - Для установки компонентов АРМ подсистемы *Интернет-Клиент* из дистрибутива запустите файл `bssetup.exe` со сменного носителя, содержащего дистрибутив подсистемы.
  - Для установки / обновления компонентов АРМ клиента подсистемы *Интернет-Клиент* с сайта банка выполните следующие действия.
    1. Наберите в адресной строке браузера адрес сайта, выданного банком. Например, "`https://bank.ru`".
    2. Откроется главная страница сайта. Также на экране отобразится окно загрузки компонентов ActiveX.

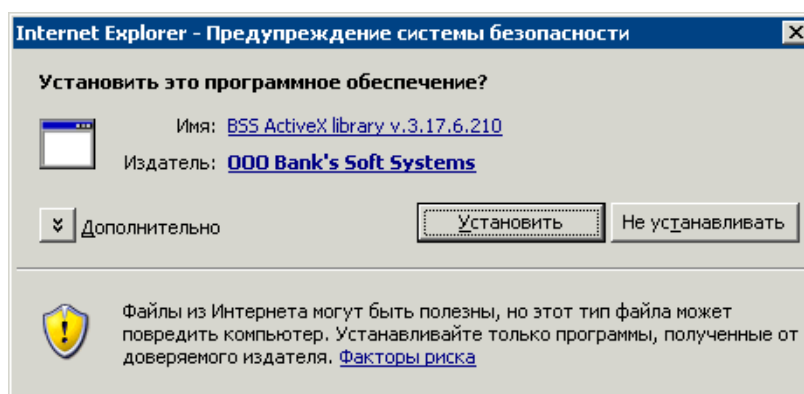


Рис. 2.10. Окно загрузки компонентов

3. Нажмите кнопку **Установить (Setup)**.
4. Появится окно выбора языка компонентов.

## Инструкции по подготовке АРМ

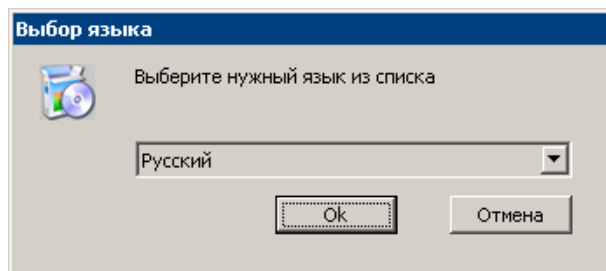


Рис. 2.11. Выбор языка

5. Выберите из раскрывающегося списка язык установки и нажмите кнопку **Ok**.
2. В случае если на ПК пользователя не устанавливались компоненты подсистемы, то перейдите к следующему пункту инструкции. В противном случае на экране будет отображено следующее окно.

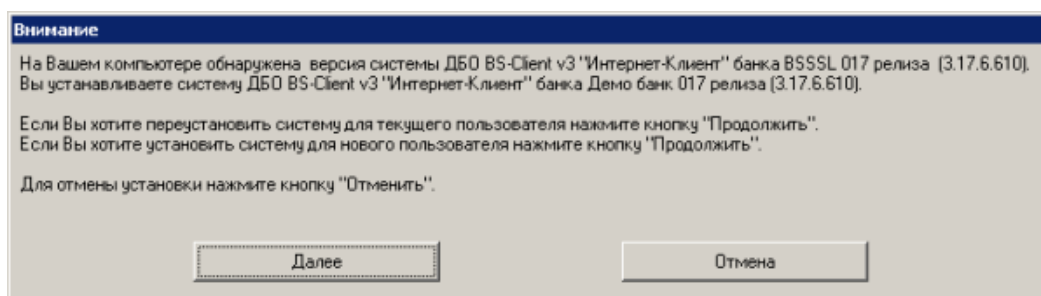


Рис. 2.12. Уведомление о наличии ранней версии

Нажмите кнопку **Далее**.

3. Произойдёт переход в главное окно мастера установки.

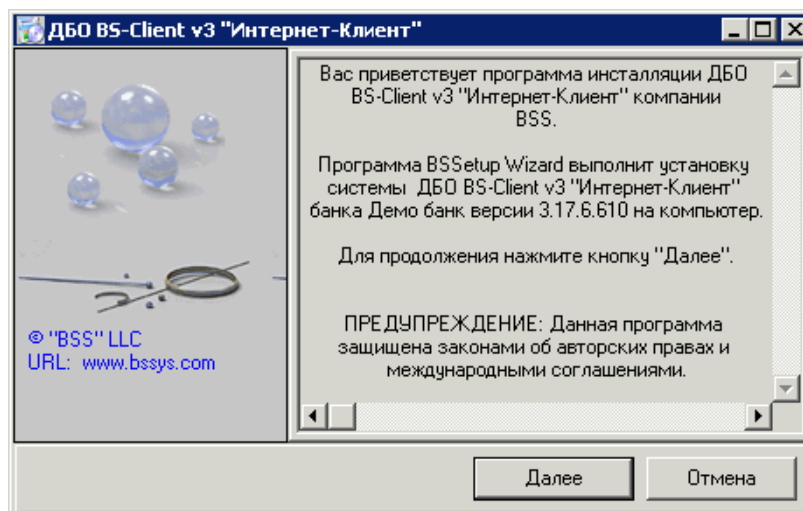


Рис. 2.13. Главное окно мастера установки

4. Нажмите кнопку **Далее**.

5. Произойдёт переход в окно выбора каталога установки.

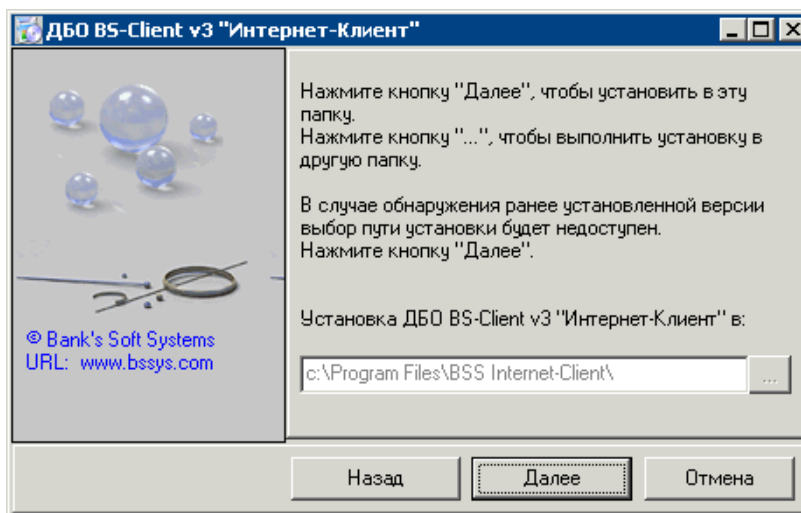


Рис. 2.14. Выбор каталога установки

6. Нажмите кнопку  и стандартным образом выберите каталог установки.

#### Примечание

В случае обнаружения ранее установленной версии выбор каталога установки будет недоступен.

7. Нажмите кнопку **Далее**.
8. Система осуществит установку компонентов и на экране появится сообщение об успешной установке подсистемы.

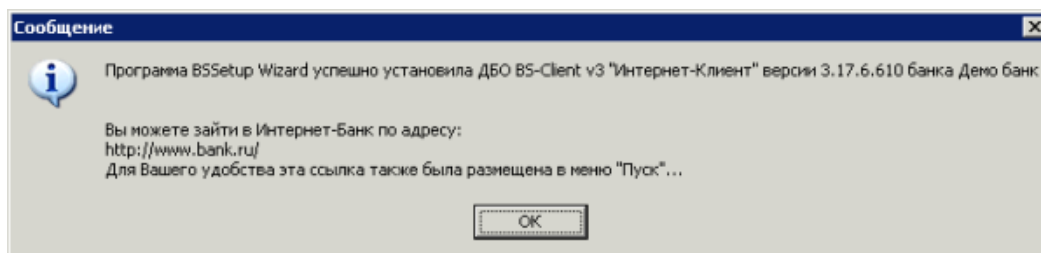


Рис. 2.15. Сообщение

9. Внимательно прочтите сообщение и нажмите кнопку **ОК** для завершения установки.

## 2.3. Начальная настройка подсистемы Интернет-Клиент

Начальная настройка подсистемы осуществляется после установки компонентов АРМ клиента подсистемы *Интернет-Клиент* (см. разд. 1.3 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 8]).

### 2.3.1. Начальная настройка параметров входа в систему с типом защиты канала односторонний SSL

При первом входе в систему пользователю необходимо настроить параметры, отвечающие за расположение криптографических ключей. Для этого:

1. В соответствии с п. 1 док. *Руководство пользователя* - п. 4 док. *Руководство пользователя* инстр. «Вход в систему с защитой канала односторонний SSL» док. *Руководство пользователя* осуществите выбор организации, от имени которой вы работаете, и подразделения, в котором осуществляется обслуживание организации.
2. На странице **Дополнительная авторизация** выполните настройку параметров, отвечающих за расположение криптографических ключей.

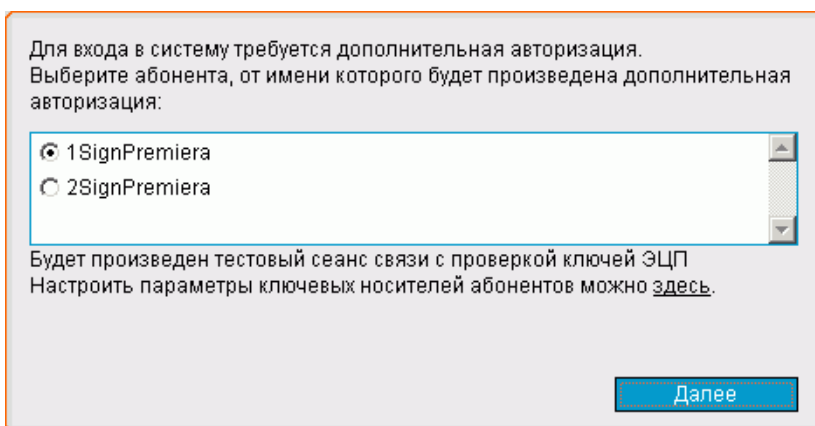


Рис. 2.16. Страница **Дополнительная авторизация**

- a. В блоке выбора задайте название абонента ЭЦП, от имени которого будет выполняться дополнительная авторизация.
- b. Выполните настройку параметров ключевых носителей.
  - i. Нажмите левой кнопкой мыши на ссылке для настройки параметров ключевых носителей.
  - ii. Откроется окно **Настройка параметров ключевых носителей абонентов ЭЦП**.

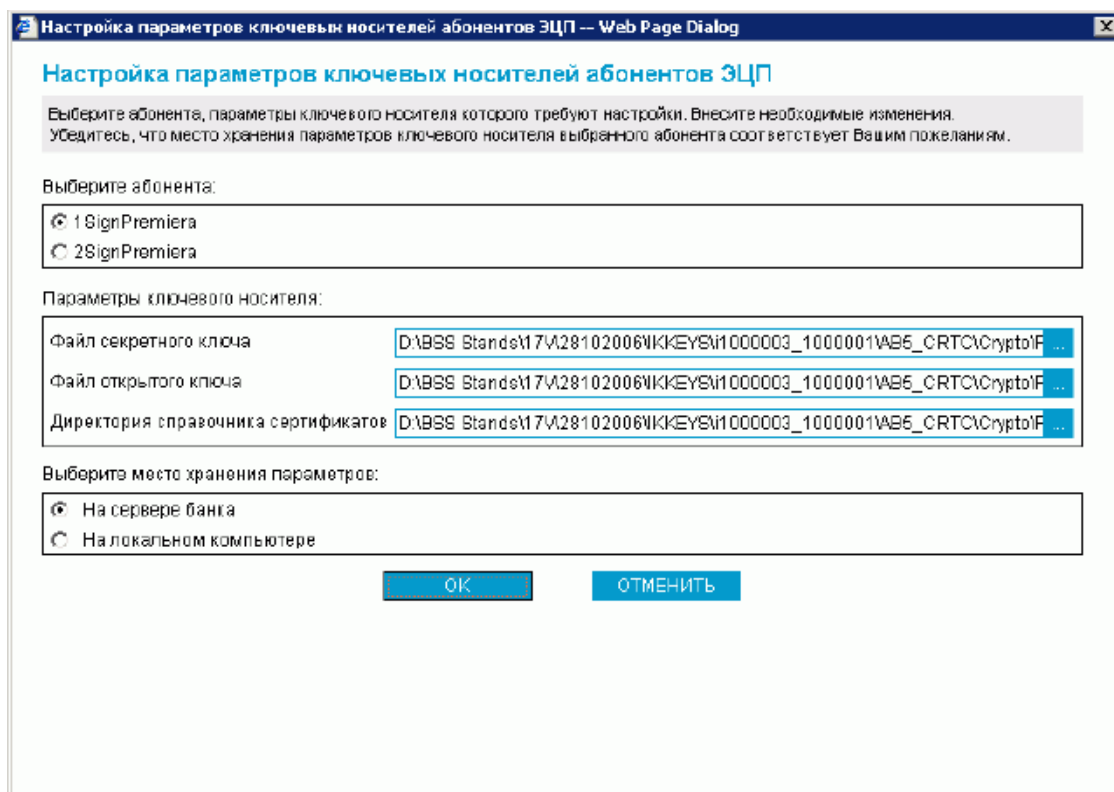


Рис. 2.17. Окно Настройка параметров ключевых носителей абонентов ЭЦП

- iii. В блоке выбора **Выберите абонента** выберите название абонента ЭЦП, для которого Вы хотите выполнить редактирование места хранения и параметры ключевого носителя абонента.
- iv. В блоке **Параметры ключевого носителя** укажите расположение файлов ключевого набора СКЗИ. Набор полей, представленных в блоке **Параметры ключевого носителя**, зависит от вида СКЗИ пользователя. Подробнее см. прил. А «Параметры СКЗИ, доступные для редактирования» [стр. 29].

#### Примечание

В ряде случаев сертификаты (открытые ключи) могут храниться не на сменных носителях, а в БД системы и считываться оттуда на лету при необходимости. В этом случае задавать расположение файла открытого ключа и расположение каталога справочника сертификатов не нужно.

- v. В блоке выбора **Выберите место хранения параметров** задайте способ хранения параметров абонента ЭЦП.
  - Для того чтобы данные параметры хранились в базе данных банка выберите значение "На сервере банка". Они будут храниться на сервере ДБО в настройках активного сертификата в криптопрофиле указанного абонента.
  - Для того чтобы настройки хранились на текущем компьютере выберите значение "На локальном компьютере". Сохранение будет осуществляться в файле конфигурации `BssCrLoc.cfg`. Хранящиеся локально, настройки

Инструкции по подготовке АРМ

---

действуют на весь криптопрофиль в целом (то есть на любые ключи, относящиеся к данному криптопрофилю).

- vi. Нажмите кнопку **ОК**. Система выполнит проверку ключевого набора.
  - vii. В случае ввода некорректных значений параметров ключевых носителей или использования неверных ключевых наборов система выведет соответствующее сообщение об ошибке. Значения параметров блока **Параметры ключевого носителя** не будут сохранены. Вернитесь к п. 2.b.iii.
  - с. После выполнения настройки параметров ключевых носителей нажмите кнопку **Далее**.
3. Завершите Вход в систему в соответствии с п. 6 док. *Руководство пользователя* инструкции инстр. «Вход в систему с защитой канала односторонний SSL» док. *Руководство пользователя*.

# Приложение А. Параметры СКЗИ, доступные для редактирования

Для обмена информацией между системой "ДБО BS-Client" и БС "1С: Предприятие" предопределенными являются следующие установки:

## А.1. Excellence 4.0

- **Директория секретного ключа / Secret key directory** – путь к каталогу, в котором хранится файл секретного ключа (abonent.key);
- **Директория открытого ключа / Public key directory** – путь к каталогу, в котором хранится файл каталога открытых ключей (catalog.key);
- **Рабочая директория / Work directory** – путь к рабочему каталогу Excellence.

## А.2. Crypto-C

- **Файл секретного ключа / User Secret key** – путь к каталогу, в котором хранится файл секретного ключа (файл с расширением .sec);
- **Файл открытого ключа / User PKey / Certificate** – путь к каталогу, в котором хранится файл открытого ключа (файл с расширением .pub);
- **Директория справочника сертификатов / Abonents dir** – путь к каталогу, в котором хранятся файлы открытых ключей Ваших абонентов.

## А.3. Crypto COM/2.2

- **Директория секретного ключа / Secret Path** – путь к каталогу, в котором хранится секретный ключ;
- **Открытый ключ / Current user certificate** – полный путь к файлу открытого ключа;
- **Директория открытых ключей абонентов / Public Path** – путь к каталогу, в котором хранятся открытые ключи Ваших абонентов;
- **Файл СЧ / Random file** – полный путь к файлу вектора инициализации датчика случайных чисел (@rand).

## А.4. OpenSSL

- **Файл секретного ключа / User Secret key** – полный путь к файлу секретного ключа;
- **Файл открытого ключа / User Certificate** – полный путь к файлу сертификата (открытого ключа);

- **Директория справочника сертификатов / Abonents dir** – путь к каталогу, в котором хранятся сертификаты абонентов ЭЦП;
- **Директория сертификата ЦА / CA dir** – путь к каталогу, в котором хранится сертификат Центра Авторизации;
- **Директория списков отозванных сертификатов / CRL dir** – путь к каталогу, в котором хранятся файлы списков отозванных сертификатов;
- **Файл СЧ / RND file** – полный путь к файлу вектора инициализации датчика случайных чисел (@rand).

## A.5. Verba-OW/4

- **Ключевое устройство / Key device** – тип ключевого устройства;
- **Директория секретного ключа / Path to secret** – путь к каталогу, в котором хранится секретной ключ;
- **Директория открытого ключа / Path to public** – путь к каталогу, в котором хранятся открытые ключи.

## A.6. CryptoPro CSP/1.1

- **Файл личного сертификата / User certificate file** – полный путь к файлу Вашего сертификата;
- **Директория сертификатов ЦС / CA certificates dir** – путь к каталогу, в котором хранятся сертификаты корневых Центров Сертификации;
- **Директория сертификатов абонентов / Abonents certificates dir** – путь к каталогу, в котором хранятся сертификаты Ваших абонентов;
- **Директория списков отозванных сертификатов / CRL dir** – путь к каталогу, в котором хранятся списки отозванных сертификатов.

## A.7. Ms Crypto API 2.0

### Примечание

Данный тип криптозащиты используется для следующих СКЗИ: Crypto Pro CSP 2.0, Crypto Pro CSP 3.0, Crypto Pro CSP 3.6.

- **Файл личного сертификата / User certificate file** – полный путь к файлу Вашего сертификата;
- **Директория сертификата ЦА / CA certificates dir** – путь к каталогу, в котором хранится сертификат Центра Авторизации;
- **Директория справочника сертификатов / Abonents certificates dir** – путь к каталогу, в котором хранятся сертификаты абонентов ЭЦП;

- **Директория списков отозванных сертификатов / CRL dir** – путь к каталогу, в котором хранятся списки отозванных сертификатов.

## A.8. LAN Crypto/2.35

- **Файл секретного ключа подписи / Sign private key** – полный путь к файлу секретного ключа подписи;
- **Файл справочника открытых ключей подписи / Sign vault** – полный путь к файлу справочника открытых ключей подписи;
- **Файл секретного ключа обмена (шифрования) / Encrypt private key** – полный путь к файлу секретного ключа обмена (шифрования);
- **Файл справочника открытых ключей обмена (шифрования) / Encrypt vault** – полный путь к файлу справочника открытых ключей обмена (шифрования);
- **Порт Touch Memory / Touch memory port number** – номер COM-порта touch memory (таблетки).

## A.9. Message-PRO 1.1, 1.3x, 2.x, 3.x

- **Файл личного сертификата / Current certificate** – полный путь к файлу Вашего сертификата;
- **Каталог сертификатов Ваших абонентов / Certificate directory** – путь к каталогу, в котором хранятся сертификаты абонентов ЭЦП;
- **Каталог секретных ключей / Private disk directory** – полный путь к файлу Вашего открытого ключа;
- **Каталог генерации новых ключей / New Keys Path** – для выполнения регенерации ключей настройка утилиты **AdminPKI** должна соответствовать значению данного параметра;
- **Каталог сертификатов центров сертификации / CA directory** – путь к каталогу, в котором хранятся сертификаты центров сертификации; в случае пустого значения за указанный каталог принимается <Private disk/directory>\CA;
- **Каталог списков отозванных сертификатов / CRL directory** – путь к каталогу, в котором хранятся списки отозванных сертификатов; в случае пустого значения за указанный каталог принимается <Private disk/directory>\CRL.

## A.10. Крипто-КОМ 3.2

- **Укажите полный путь к файлу Вашего открытого ключа** – путь к каталогу, в котором хранится файл;
- **Укажите полный путь к каталогу Вашего секретного ключа** – путь к каталогу, в котором хранится секретный ключ (набор файлов `masks.db3`, `kek.opq`, `rand.opq`, `mk.db3`, подкаталог KEYS);

- **Укажите директорию, в которой находятся открытые ключи Ваших абонентов** – путь к каталогу, в котором хранятся файлы открытых ключей Ваших абонентов (файлы с расширением .pub).

## A. 1 1. Агава-С

- **Файл открытого ключа / Public key file** – полный путь к файлу вашего открытого ключа;
- **Каталог секретных ключей / Private keys folder** – каталог с Вашими секретными ключами;
- **Каталог справочника сертификатов / Folder for the register of certificates** – каталог, в котором находятся файлы открытых ключей Ваших абонентов.