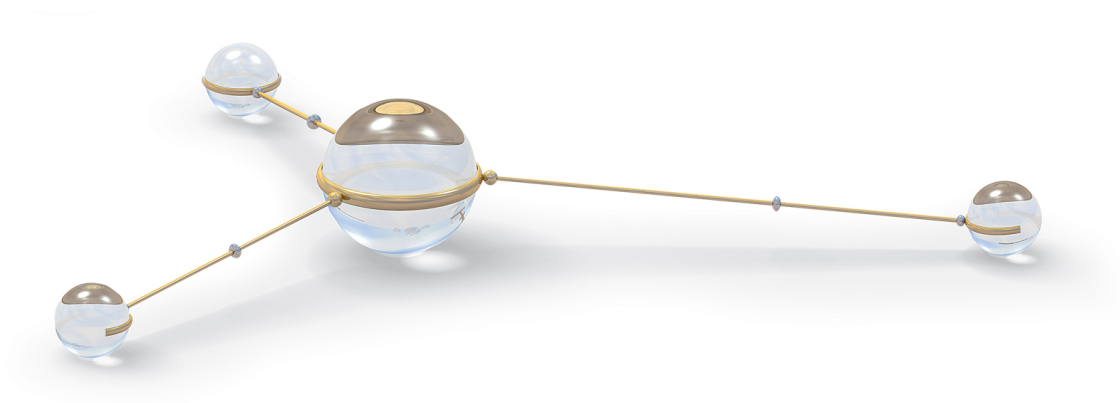




Система "ДБО BS-Client x64"

Версия 20.1.730. Централизованная и Распределенная
СХЕМЫ
Документация клиента "Интернет-Клиент".

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



Система "ДБО BS-Client x64"

Версия 20.1.730. Централизованная и Распределенная схемы

Документация клиента "Интернет-Клиент".

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

Опубликовано 2016

Листов 31

© 2016 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 x64" ("ДБО BS-Client x64") 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.

© 2016 ООО "БСС"

Содержание

Введение	4
Глоссарий	6
1. Общие сведения	9
1.1. Обеспечение безопасности данных	9
1.1.1. Защита ключей	9
1.2. Требования к программному окружению	9
1.2.1. Требования к программному окружению	10
1.3. Требования к аппаратному обеспечению	11
1.4. Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент	11
1.5. Описание процесса обновления компонентов АРМ клиента	12
1.6. Особенности использования браузеров и ОС различных версий	12
1.6.1. Особенности работы с ОС Windows Vista	12
1.6.2. Особенности печати документов в Internet Explorer	14
1.6.3. Особенности масштабирования в браузерах Internet Explorer, Opera и Google Chrome	14
1.6.4. Особенности установки АРМ клиента подсистемы Интернет-Клиент на виртуальных машинах	15
2. Инструкции по подготовке АРМ	16
2.1. Настройка сопутствующего ПО	16
2.1.1. Настройка браузера Internet Explorer	16
2.1.2. Настройка Windows Vista	22
2.2. Установка / обновление компонентов АРМ клиента подсистемы Интернет-Клиент	25
2.3. Начальная настройка подсистемы Интернет-Клиент	27
2.3.1. Начальная настройка параметров входа в систему с типом защиты канала односторонний SSL	27
А. Параметры СКЗИ, доступные для редактирования	30
А.1. OpenSSL	30
А.2. Ms Crypto API 2.0	30
А.3. Message-PRO 1.3x, 2.x, 3.x	30

Введение

Настоящий документ является частью документации по системам "ДБО BS-Client x64" версии 20.1.730, функционирующим в режимах Централизованной и Распределенной схем.

На кого ориентирован документ

Документ предназначен для пользователя клиентской части подсистемы "Интернет-Клиент".

Назначение документа

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

Организация документа

Документ разбит на несколько глав.

В гл. 1 «Общие сведения» [стр. 9] приводится общая информация о подсистеме *Интернет-Клиент*.

В гл. 2 «Инструкции по подготовке АРМ» [стр. 16] 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 x64". Документ рекомендован как для последовательного, так и для выборочного изучения.

Внимание!

Материал может содержать большое количество перекрестных ссылок на другие части документации. Для интенсивного изучения материала, быстрого поиска необходимой информации и удобного перехода по ссылкам рекомендуется воспользоваться контекстной справкой системы "ДБО BS-Client x64": в справке содержится наиболее полная информация о системе и порядке работы с ней. Контекстная справка вызывается из системы по нажатию клавиши **F1**.

Соглашения по оформлению

Кавычками выделяются значения полей экранных форм и различных параметров.

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

Ссылки в тексте снабжены подчеркиванием.

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

Гл.	Глава (документа).
Гр.инстр.	Группа инструкций. См. также Инструкция.
ДБО	Дистанционное банковское обслуживание. См. также Централизованная система "ДБО BS-Client x64", Распределенная система "ДБО BS-Client x64".
Инстр.	См. Инструкция.
ОС	Операционная система.
ПО	Программное обеспечение.
РС	См. Распределенная система "ДБО BS-Client x64".
Разд.	Раздел (документа).
ЦС	См. Централизованная система "ДБО BS-Client x64".

Перечень терминов

Web-банк	Собирательное понятие, используемое для обозначения совокупности подсистем <i>Web-интерфейс администратора</i> и <i>Web-интерфейс оператора</i> .
Банк-клиент	<i>Подсистема</i> , предназначенная для пользователей-клиентов банка, обеспечивающая взаимодействие пользователя с системой посредством устанавливаемого на рабочей станции пользователя клиентского приложения Sbank .
Банковская часть системы (подсистемы)	Совокупность компонентов системы (подсистемы), расположенных на <i>стороне банка</i> .
Выписка Он-Лайн	<i>Подсистема</i> , являющаяся ограниченным вариантом подсистемы <i>Интернет-Клиент</i> . Предоставляет клиентам банка функционал просмотра выписок по своим счетам и информационных сообщений, без возможности осуществления каких-либо финансовых транзакций.
Инструкция	В рамках документации по системе "ДБО BS-Client x64" инструкция (сокращенно <i>инстр.</i>) – подробное описание последовательности действий, которые необходимо выполнить в системе "ДБО BS-Client x64" 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 докумен-

Глоссарий

	та, подпись документа, изменение пароля для входа в систему. Порядок выполнения инструкций определяется <i>регламентами</i> по работе с системой.
Интернет-клиент	<i>Подсистема</i> , предназначенная для пользователей-клиентов банка, обеспечивающая взаимодействие пользователя с системой посредством веб-браузера.
Клиент	Юридическое лицо, индивидуальный предприниматель или физическое лицо, занимающееся частной практикой в порядке, установленном действующим законодательством Российской Федерации, заключившее с банком договор на предоставление услуг с использованием системы "ДБО BS-Client x64" (см. разд. 2.1 «Бизнес-структура системы» док. <i>Интернет-Клиент. Руководство пользователя</i>).
Клиентская часть системы (подсистемы)	Совокупность компонентов системы (подсистемы), расположенных на <i>стороне клиента</i> .
Подразделение	Обособленное (филиал) либо внутреннее структурное подразделение кредитной организации, имеющее право принимать платежно-расчетные документы юридических лиц. В рамках системы "ДБО BS-Client x64", работающей в режиме <i>Централизованной схемы</i> , могут взаимодействовать несколько подразделений, одно из которых является головным; в рамках системы, работающей в режиме <i>Распределенной схемы</i> , присутствует единственное подразделение. К подразделению может относиться несколько удаленных площадок. См. также Головное подразделение.
Подсистема	Совокупность компонентов системы, предназначенных для решения определенных технологических задач. Подсистемы делятся на <i>основные подсистемы</i> и <i>служебные подсистемы</i> .
Распределенная система "ДБО BS-Client x64"	Децентрализованный режим работы системы "ДБО BS-Client x64", при котором хранение данных, учет клиентов и документооборот осуществляются отдельно в каждом филиале кредитной организации и независимо от других филиалов.
Сторона банка	Совокупность комплекса (АРМ) банка и комплексов удаленных площадок.
Сторона клиента	Совокупность комплексов (АРМ) клиента.
Учетная запись пользователя	Объект системы "ДБО BS-Client x64", содержащий аутентификационные данные пользователя, а также другую информацию, необходимую для разграничения доступа пользователей к системе.
Централизованная система "ДБО BS-Client x64"	Режим работы системы "ДБО BS-Client x64", при котором управление системой, хранение данных, учет клиентов и документооборот централизованы в головном подразделении многофилиального банка. При использовании данного режима работы весь документооборот между



Глоссарий

клиентами и филиалами банка осуществляется через сервер ДБО, расположенный в головном подразделении кредитной организации.

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 – ЭП) 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 жесткий 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 программному окружению

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

1.2.1. Требования к программному окружению

Вид ПО	Наименование ПО	Версии ПО		Примечания
		Рекоменд.	Поддерж.	
ОС	Windows	7 x86 и x64 (Ultimate, Professional, Enterprise, Home Premium, Home Basic)	Vista x86, 2008 Server (Standard Edition, Datacenter Edition, Web Edition), 2012 Server x64 (Foundation Edition, Essentials Edition, Standard Edition, Datacenter Edition), 8 x86 и x64 (8, 8 Pro, 8 Enterprise) 10 x86 и x64 (Home, Professional, Enterprise)	Для работы с ОС Windows Vista требуется специальная настройка ОС
Средства виртуализации	VMware vSphere	4.1, 5.1		
	Microsoft Hyper-V	Server 2008, Server 2008 R2, Server 2012, Server 2012 R2		
	Oracle VM Virtual Box 4.0			
	Parallels Desktop 6 для Mac			
	Citrix XenServer 5.6			
Веб-браузер	Microsoft Internet Explorer x86, x64	9.0, 10.0, 11.0		
	Mozilla Firefox x86	24.0		
	Opera x86	Next 17.x		
	Google Chrome x86	29.x		

Вид ПО	Наименование ПО	Версии ПО		Примечания
		Рекоменд.	Поддерж.	
ПО для работы с документацией	Один из продуктов компании Adobe			

1.3. Требования к аппаратному обеспечению

Компьютер, с которого будет осуществляться работа, должен обладать характеристиками не ниже следующих:

1. процессор Pentium 166;
2. объем оперативной памяти 32 Mb;
3. объем свободного места на диске 50Mb;
4. прямой доступ в интернет с шириной канала 512 кб/с и выше;
5. видеосистема, обеспечивающая область экрана не менее 1024x768 пикселей.

1.4. 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 программному окружению» [стр. 9]. При выборе версий стороннего ПО необходимо руководствоваться особенностями использования ПО (см. разд. 1.6 «Особенности использования браузеров и ОС различных версий» [стр. 12]).
 - 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.
 - c. Для настройки СПО выполните действия, описанные в гр. инстр. «Настройка сопутствующего ПО» [стр. 16].

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. 25].
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. 27].

1.5. Описание процесса обновления компонентов АРМ клиента

Обновление компонентов АРМ клиента подсистемы *Интернет-Клиент* инициируется на стороне банка. Если на сервере банка появился пакет обновлений АРМ, то при входе на главную страницу сайта или после входа в подсистему будет предложено установить плагин, обеспечивающий работу клиентской части подсистемы *Интернет-Клиент*. Для того чтобы установить плагин выполните действия, описанные в инстр. «Установка / обновление компонентов АРМ клиента подсистемы Интернет-Клиент» [стр. 25].

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.

1.6. Особенности использования браузеров и ОС различных версий

1.6.1. 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.

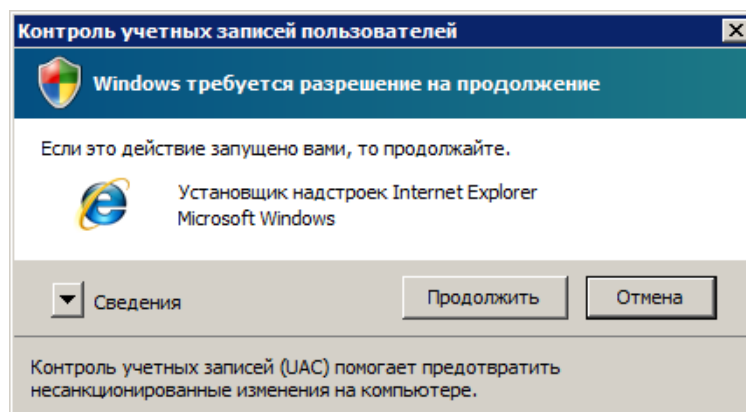


Рис. 1.1. Запрос UAC подтверждения необходимости выполнения действия

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 при входе на сайт плагина, обеспечивающего работу клиентской части подсистемы *Интернет-Клиент*. 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. 12.4 «Настройка параметров ключевых носителей абонентов ЭП»](#) док. *Интернет-Клиент. Руководство пользователя*), либо отключение UAC (см. [инстр. «Настройка Windows Vista»](#) [стр. 22]).

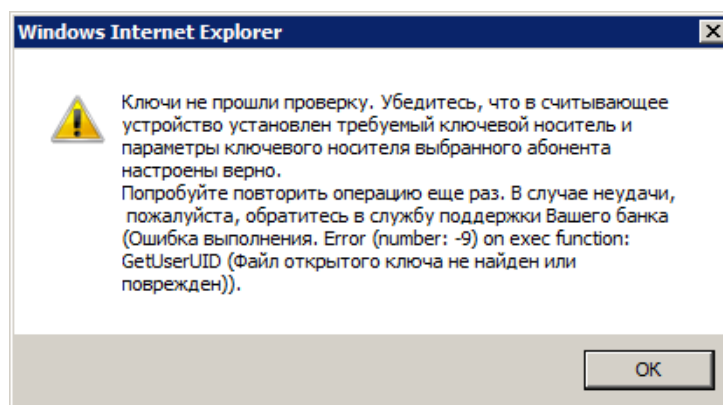


Рис. 1.2. Сообщение, возникающее при запрете UAC обращения к криптографическим ключам

- Сохранение параметров ключевых носителей локально в файле на жестком диске (см. [разд. 12.4 «Настройка параметров ключевых носителей абонентов ЭП»](#) док. *Интер-*

нет-Клиент. Руководство пользователя). При попытках сохранения параметров на жестком диске UAC запрещает обращение к диску. В этом случае также необходимо либо размещение файла с параметрами ключевых носителей на сменных носителях, либо отключение UAC (см. инстр. «Настройка Windows Vista» [стр. 22]).

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. 22].

1.6.2. 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. 13 - п. 20 инстр. «Настройка браузера Internet Explorer» [стр. 16].

Примечание

При использовании браузера Internet Explorer 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/>.

1.6.3. Особенности масштабирования в браузерах Internet Explorer, Opera и Google Chrome

В случае неправильного выбора масштаба веб-страниц в браузерах Internet Explorer, Opera и Google Chrome возможны следующие ошибки и нестандартные ситуации:

- В браузере Internet Explorer отдельные из полей некоторых видов документов могут отображаться некорректно.
- В браузерах Opera и Google Chrome может быть недоступно изменение размера области навигации.

Для корректного отображения веб-страниц необходимо перед началом работы в браузерах Internet Explorer, Opera и Google Chrome установить масштаб "100%".

1.6.4. Особенности установки *АРМ* клиента подсистемы *Интернет-Клиент* на виртуальных машинах

В случае если планируется выполнить установку *АРМ* клиента подсистемы *Интернет-Клиент* на виртуальной машине, необходимо предварительно обеспечить:

1. Доступ виртуальной машины к сети Интернет.
2. Доступ к носителям ключевой информации USB-токен.

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. 1.4 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 11]).

2.1.1. Настройка браузера Internet Explorer

Для настройки браузера Internet Explorer:

1. Стандартным образом откройте браузер Internet Explorer.
2. Выберите пункт меню **Сервис (Tools)** → **Свойства обозревателя (Internet Options)**.
3. Откроется окно **Свойства Обозревателя (Internet Options)**.
4. Перейдите к вкладке **Безопасность (Security)**.

Инструкции по подготовке АРМ

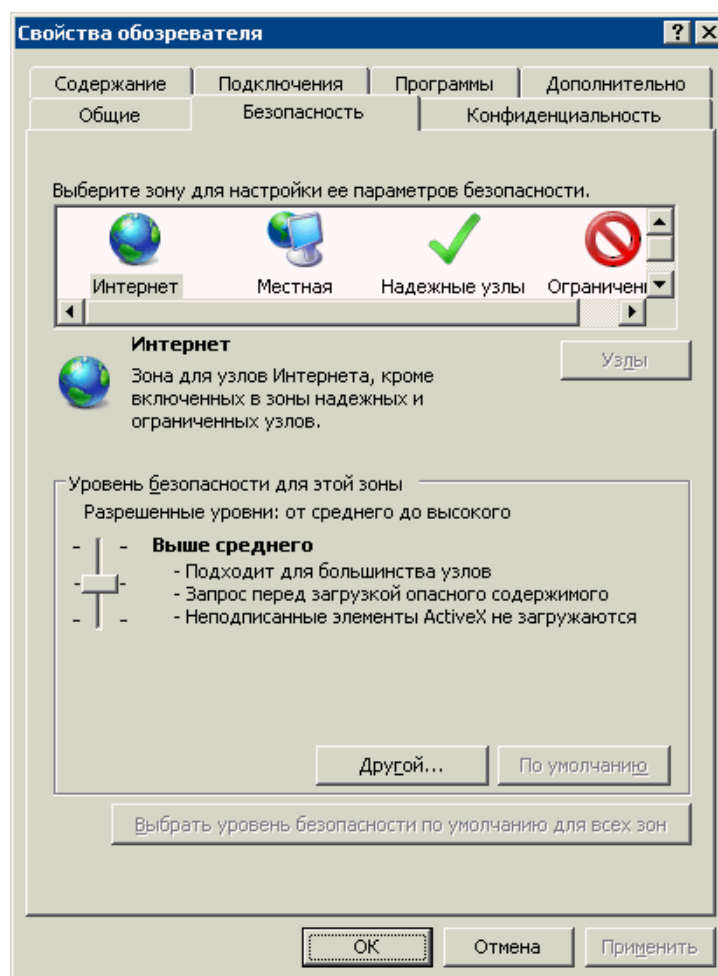


Рис. 2.1. Вкладка безопасность окна Свойства обозревателя браузера Internet Explorer 7.0

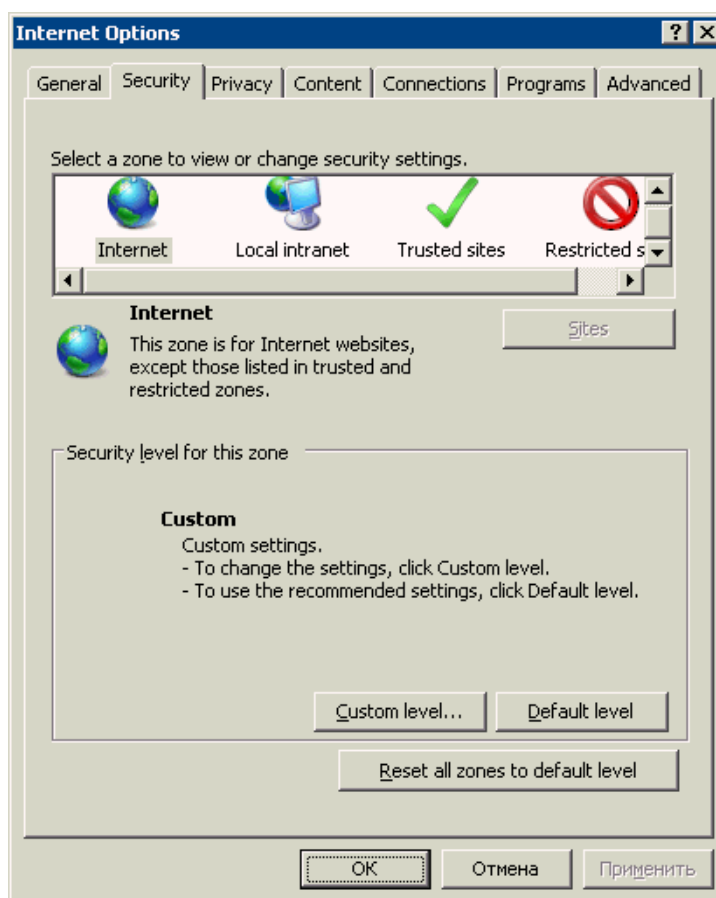


Рис. 2.2. Вкладка безопасность окна Свойства обозревателя браузера Internet Explorer 8.0

5. Выберите зону "Интернет" ("Internet") для настройки ее 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)**.

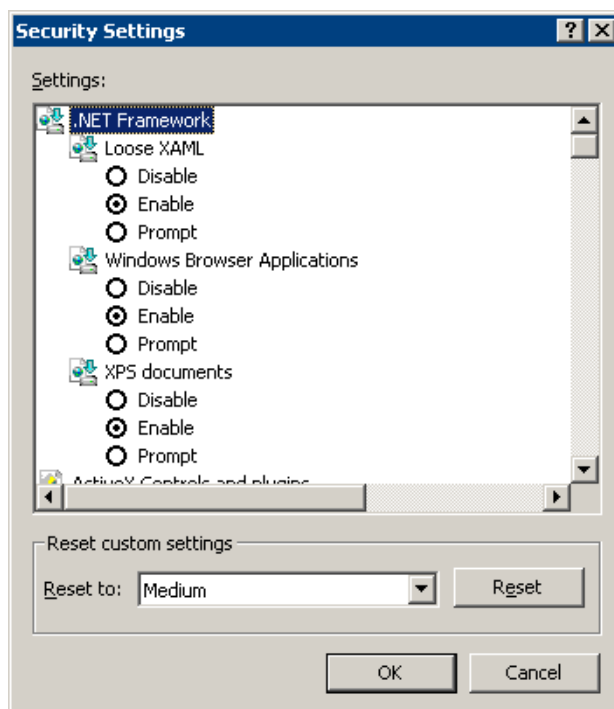


Рис. 2.3. Окно Правила безопасности

8. В блоке **Параметры (Settings)** заполните поля параметров согласно значениям, приведенным 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. При необходимости добавьте адрес сайта банка в список доверенных сайтов:
 - a. Перейдите к вкладке **Безопасность (Security)** окна **Свойства Обозревателя (Internet Options)**.
 - b. Выберите зону "Доверенные сайты" ("Trusted sites") и нажмите кнопку **Узлы (Sites)**.
 - c. В открывшемся окне в поле ввода введите адрес сайта банка и нажмите кнопку **Добавить (Add)**.
 - d. Закройте окно.
11. Настройте дополнительные параметры безопасности:
 - a. Перейдите к вкладке **Дополнительно (Advanced)** окна **Свойства Обозревателя (Internet Options)**.
 - b. В блоке **Параметры (Settings)** заполните поля выбора **SSL2.0 (Use SSL2.0)** и **SSL3.0 (Use SSL3.0)** группы **Безопасность (Security)**.
12. Нажмите последовательно кнопку **Применить (Apply)**, затем кнопку **ОК** для сохранения внесенных изменений.
13. Выберите пункт меню **Файл (File)** → **Параметры страницы (Page Setup)**.
14. Откроется окно **Параметры страницы (Page Setup)**.

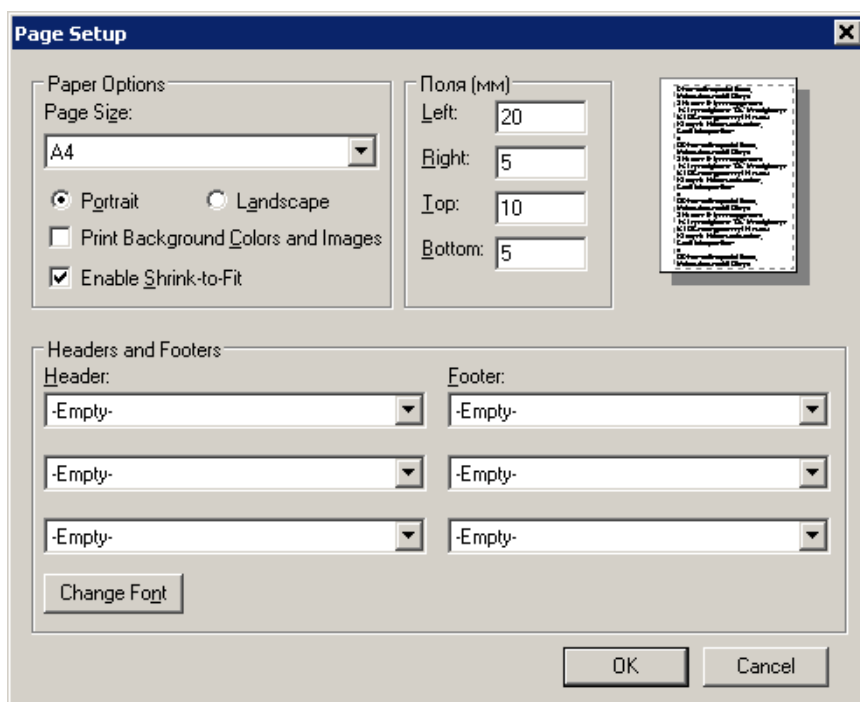


Рис. 2.4. Окно Параметры страницы (Page Setup)

15. В блоке **Параметры бумаги (Paper Options)** заполните поле выбора **Книжная (Portrait)**.
16. Для полей блока **Поля (мм) (Margins (millimeters))** установите следующие значения:
 - a. **Левое (Left)** – не более " 20 ";
 - b. **Правое (Right)** – не более " 5 ";
 - c. **Верхнее (Top)** – не более " 10 ";
 - d. **Нижнее (Bottom)** – не более " 5 ".
17. Во всех полях выбора блока **Колонтитулы (Headers and Footers)** выберите значение " -Пусто- " (" -Empty- ").
18. В некоторых версиях браузера Internet Explorer реализована возможность уменьшения размеров печатаемого документа до размеров страницы. Данная функция должна быть отключена. Для отключения функции сжатия снимите заполнение поля **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. 1.6.2 «Особенности печати документов в Internet Explorer»](#) [стр. 14].

19. Для прочих параметров оставьте значения по умолчанию.
20. Нажмите кнопку **ОК** для сохранения внесенных изменений.

2.1.2. Настройка Windows Vista

В случае использования ОС Windows Vista рекомендуется отключить механизм контроля учетных записей (см. [разд. 1.6.1 «Особенности работы с ОС Windows Vista»](#) [стр. 12]).

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

1. Отобразите панель управления Windows (Control Panel).

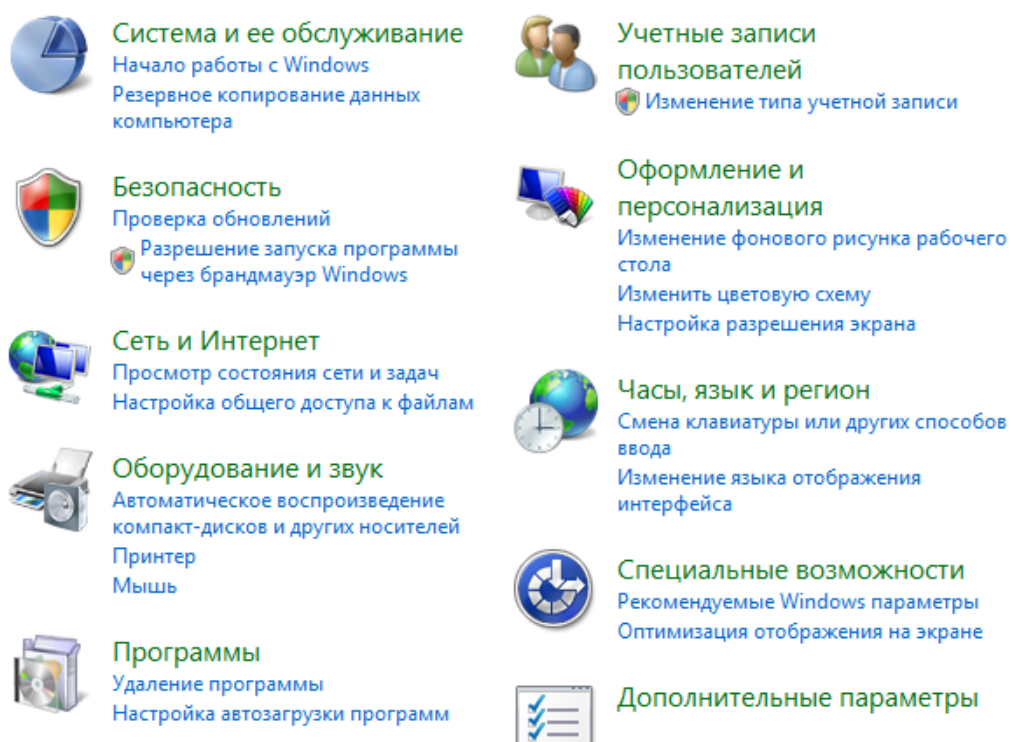


Рис. 2.5. Фрагмент панели управления Windows

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

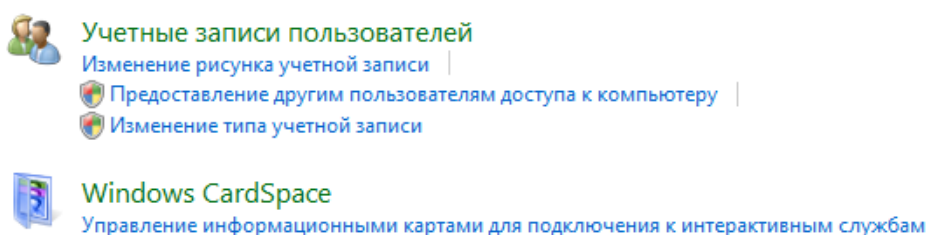


Рис. 2.6. Окно настройки учетных записей пользователей

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

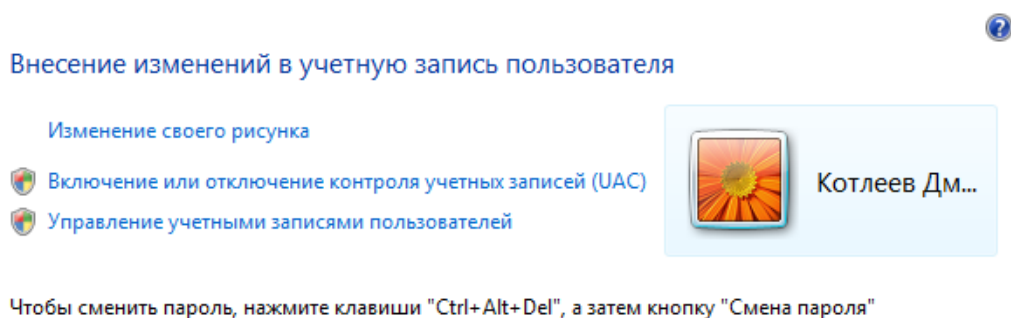


Рис. 2.7. Окно изменения параметров учетной записи пользователя

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. 2.8. 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. 1.4 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 11]).

В процессе установки компонентов подсистемы *Интернет-Клиент* на этапе дополнительной авторизации в случае использования браузера Internet Explorer 9.0 может потребоваться установка сертификата от центра сертификации банка.

Обновление компонентов АРМ клиента подсистемы может осуществляться только с сайта банка (см. разд. 1.5 «Описание процесса обновления компонентов АРМ клиента» [стр. 12]).

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.msi` 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 с предложением установить плагин, обеспечивающий работу клиентской части подсистемы *Интернет-Клиент*.
 3. Нажмите кнопку **Загрузить Плагин**.
 4. Откроется страница установки плагина.

Примечание

При появлении диалога **Загрузка файла** нажмите кнопку **Запустить**. В случае вывода на экран предупреждения системы безопасности нажмите кнопку **Запустить / Выполнить**. В случае вывода на экран диалогового окна **Контроль учетных записей пользователей** нажмите кнопку **Да**.

2. Произойдет переход в главное окно мастера установки.

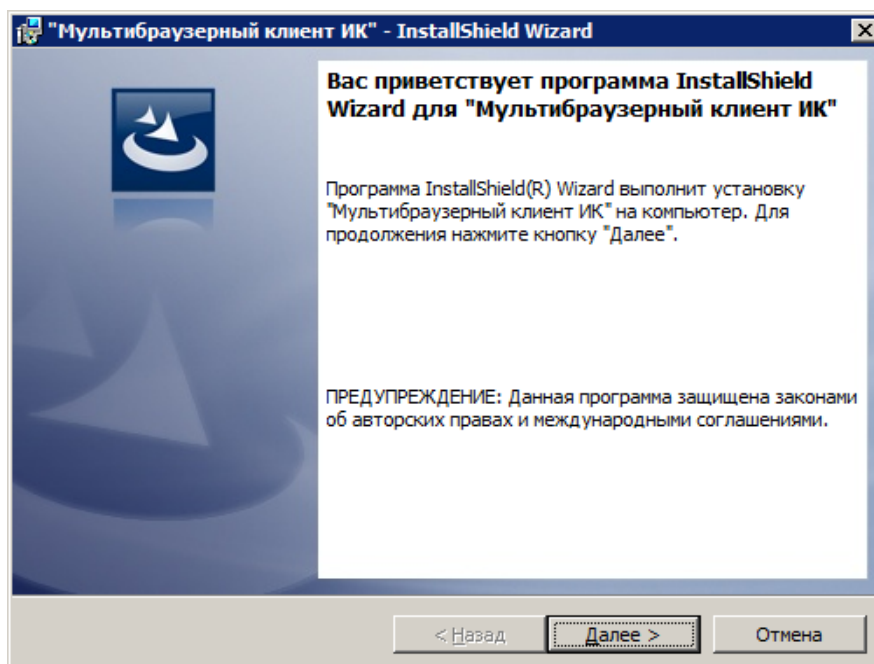


Рис. 2.9. Главное окно мастера установки плагина

3. Нажмите кнопку **Далее**.
4. Произойдет переход в окно выбора каталога установки.

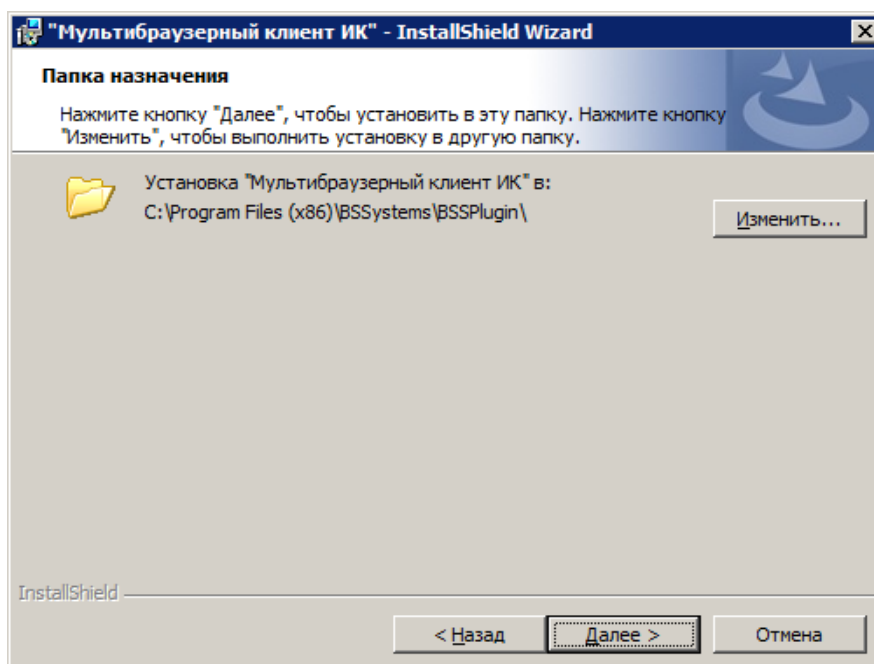


Рис. 2.10. Выбор каталога установки

5. Нажмите кнопку **Изменить** и стандартным образом выберите каталог установки.
6. Нажмите кнопку **Далее**.

7. В открывшемся окне нажмите кнопку **Установить**.
8. Система осуществит установку плагина и на экране появится сообщение об успешной установке.
9. Прочтите сообщение и нажмите кнопку **Готово** для завершения установки.

2.3. Начальная настройка подсистемы Интернет-Клиент

Начальная настройка подсистемы осуществляется после установки компонентов АРМ клиента подсистемы *Интернет-Клиент* (см. разд. 1.4 «Описание процесса подготовки АРМ клиента подсистемы Интернет-Клиент» [стр. 11]).

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. *Интернет-Клиент. Руководство пользователя* - п. 6 док. *Интернет-Клиент. Руководство пользователя* (при работе системы в режиме ЦС) или п. 1 док. *Интернет-Клиент. Руководство пользователя* - п. 5 док. *Интернет-Клиент. Руководство пользователя* (при работе системы в режиме РС) разд. 3.1.1 «Вход в систему с защитой канала односторонний SSL» осуществите выбор организации, от имени которой вы работаете, и подразделения, в котором осуществляется обслуживание организации (при работе системы в режиме ЦС).
2. На странице **Дополнительная авторизация** выполните настройку параметров, отвечающих за расположение криптографических ключей.

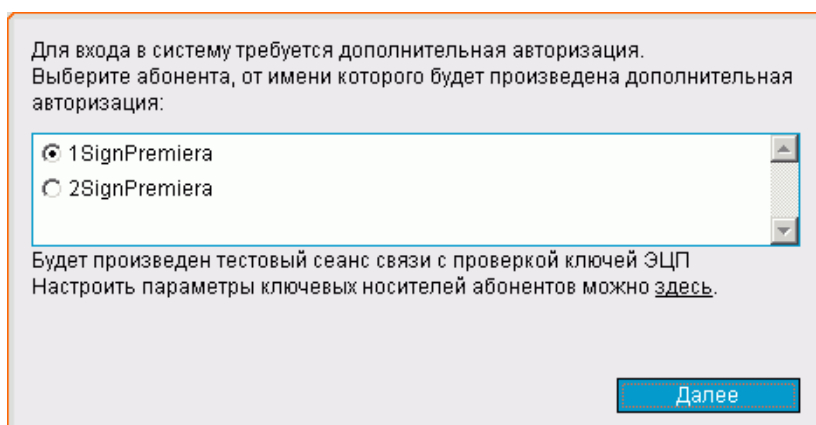


Рис. 2.11. Страница **Дополнительная авторизация**

- a. В блоке выбора укажите название абонента ЭП, от имени которого будет выполняться дополнительная авторизация.
- b. Выполните настройку параметров ключевых носителей.

Инструкции по подготовке АРМ

- А. Нажмите левой кнопкой мыши на ссылке для настройки параметров ключевых носителей.
- В. Откроется окно **Настройка параметров ключевых носителей абонентов ЭП**.

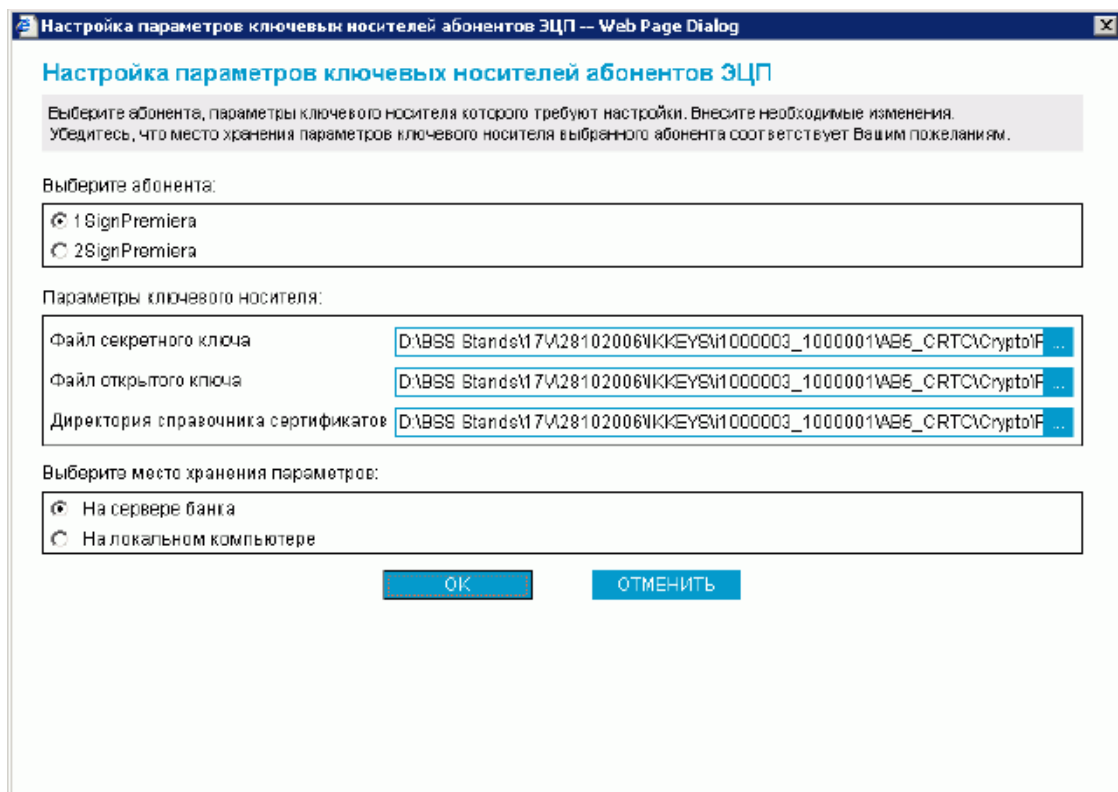


Рис. 2.12. Окно Настройка параметров ключевых носителей абонентов ЭП

- С. В блоке выбора **Выберите абонента** выберите название абонента ЭП, для которого Вы хотите выполнить редактирование места хранения и параметры ключевого носителя абонента.
- Д. 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. 30].

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.

- Е. В блоке выбора **Выберите место хранения параметров** задайте способ хранения параметров абонента ЭП.

Инструкции по подготовке АРМ

- 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 действуют на весь криптопрофиль в целом (то есть на любые ключи, относящиеся к данному криптопрофилю).
- Ф. Нажмите кнопку **ОК**. Система выполнит проверку ключевого набора.
- Г. 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.б.С.
- с. После выполнения настройки параметров ключевых носителей нажмите кнопку **Далее**.
3. Завершите Вход в систему в соответствии с п. 8 док. *Интернет-Клиент. Руководство пользователя* инструкции разд. 3.1.1 «Вход в систему с защитой канала односторонний SSL».

Приложение А. Параметры СКЗИ, доступные для редактирования

Для обмена информацией между системой "ДБО BS-Client x64" и БС "1С: Предприятие" предопределенными являются следующие установки:

А.1. 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 ЭП;
- **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).

А.2. 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 ЭП;
- **Директория списков отозванных сертификатов / CRL dir** – путь к каталогу, в котором хранятся списки отозванных сертификатов.

А.3. Message-PRO 1.3x, 2.x, 3.x

- **Файл личного сертификата / Current certificate** – полный путь к файлу Вашего сертификата;

Параметры СКЗИ, доступные для редактирования

- **Каталог сертификатов Ваших абонентов / Certificate directory** – путь к каталогу, в котором хранятся сертификаты абонентов ЭП;
- **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.