Internet-Банкинг для корпоративных клиентов. Регистрация в системе iBank 2 UA

ООО «БИФИТ Сервис»

(версия 2.0.23.29)

Оглавление

Введение

Настоящий документ представляет собой руководство по использованию модуля АРМ **Регистратор** системы электронного банкинга iBank 2 UA. Данный модуль предназначен для предварительной регистрации корпоративных клиентов и ключей ЭЦП в системе iBank 2 UA в режиме Internet-Банкинга.

В разделе **Предварительная настройка** приведены общие требования к компьютеру клиента, подключению к Интернет и другие дополнительные настройки для обеспечения корректной работы АРМ **Регистратор**.

Необходимые действия клиента для входа в АРМ **Регистратор** описаны в разделе **Вход в систему**.

Подробное описание процедуры регистрации нового корпоративного клиента и ЦФК представлено в разделе **Регистрация корпоративного клиента**.

Раздел **Регистрация ключей ЭЦП** посвящен описанию процедуры регистрации новой пары ключей ЭЦП.

В разделе **Администрирование ключей ЭЦП** представлено описание возможностей АРМ **Регистратор** по управлению ключами ЭЦП корпоративных клиентов.

Раздел 1

Предварительная настройка

Требования к системе

Для работы с системой клиенту необходимы:

1. Компьютер, удовлетворяющий следующим требованиям:

   (a) Операционная система:

   - семейства Windows: Server 2008, Server 2012 (64-разрядная версия), XP SP3 (32-разрядная версия), XP SP2 (64-разрядная версия), Vista SP2, 7, 8.
   - Mac на базе Intel, на котором запущен Mac OS X 10.7.3 (Lion) или более поздней версии.
   - Linux: Oracle Linux 5.5+, Oracle Linux 6.x (32-разрядная версия), 6.x (64-разрядная версия), Red Hat Enterprise Linux 5.5+, 6.x (32-разрядная версия), 6.x (64-разрядная версия), Ubuntu Linux 10.04 и выше, Suse Linux Enterprise Server 10 SP2, 11.x.

   (b) Оперативная память - 128 Мбайт.

   Кроме вышеперечисленных требований рекомендуется наличие в компьютере клиента USB-порта для использования съемных носителей информации. Съемный носитель информации (например, USB-токен[1]) необходим для хранения ключей ЭЦП клиента.

   Рекомендуется также наличие принтера, на котором будет распечатан Сертификат открытого ключа ЭЦП клиента.

2. Установленный Web-браузер на компьютере клиента, а также наличие Java-машины (Java Runtime Environment). В качестве Web-браузера рекомендуется использовать одну из следующих программ:

   - Microsoft Internet Explorer 7.0 и выше;
   - Google Chrome;
   - Mozilla Firefox 3.6 и выше;
   - Opera;
   - Safari;

   Для установки на компьютере клиента виртуальной Java-машины, необходимо с Web-сайта компании-разработчика (http://www.java.com) скачать и установить дистрибутив.

   Настоятельно рекомендуется использовать последнюю версию виртуальной Java-машины.

   Внимание!

   Для корректной работы под операционной системой Mac OS X необходимо использовать 64-битный браузер.

[1] Устройство, подключаемое к USB-порту компьютера, которое служит для безопасного хранения ключей ЭЦП клиента. В отличие от других съемных носителей, с USB-токена невозможно скопировать ключи ЭЦП, что существенно снижает возможность несанкционированного доступа к ключу ЭЦП клиента.

Внимание!
При установленной 64-битной виртуальной Java-машине требуется использовать 64-битный браузер.

3. Наличие установленных драйверов для USB-токенов, если клиент использует USB-токены для хранения своих секретных ключей ЭЦП. Актуальные версии драйверов поддерживаемых USB-токенов можно скачать с сайта компании-разработчика.

4. Доступ в Интернет. Рекомендуемая скорость соединения — 1 Мбит/сек. Также возможна работа и на низкоскоростных соединениях (GSM-модем (3G/GPRS), модемный пул Банка), однако при таком канале связи вместо АРМ **Регистратор** рекомендуется использовать модуль **РС-Банкинг** (описание работы модуля представлено в документации ***РС-Банкинг для корпоративных клиентов. Регистрация в системе iBank 2 UA***).

Настройка подключения к Интернет

Для работы с системой iBank 2 UA клиенту необходимо подключиться к Интернет. На практике используются несколько видов соединений с сетью Internet:

1. Модемное соединение через асимметричную цифровую абонентскую линию (ADSL);
2. Широкополосный доступ по выделенной линии (Ethernet);
3. Доступ с помощью технологии Mobile WiMAX/Wi-Fi;
4. Мобильный GPRS/3G доступ;
5. Спутниковое подключение к сети.

При подключении к сети обычно используется Firewall (межсетевой экран). Firewall осуществляет фильтрацию пакетов в соответствии с правилами, заданными администратором. Поэтому для работы Java-апплетов в правилах фильтрации на Firewall необходимо открыть следующие TCP-порты:

- TCP-порт для соединения Web-браузера клиента с Web-сервером банка по протоколу SSL (для этого соединения обычно используется порт 443);
- TCP-порт для работы Java-апплета **Регистратор** с Сервером iBank 2 UA (для этого соединения обычно используется порт 9091);

Номера TCP-портов могут быть различными для разных банков. В этом случае необходимо связаться с сотрудником банка для уточнения номеров TCP-портов, которые необходимо открыть в IP-фильтре на Firewall.

Раздел 2

Вход в систему

Для работы в системе электронного банкинга iBank 2 UA корпоративному клиенту необходимо зарегистрироваться в системе. Процесс регистрации клиента в iBank 2 UA включает в себя предварительную (через Интернет) и окончательную (в отделении банка) регистрацию.

Предварительную регистрацию в режиме Internet-Банкинг клиент может выполнить в АРМ **Регистратор**, который представляет собой Java-апплет **Регистратор**. Для загрузки Java-апплета **Регистратор** после подключения к Интернет (подробнее см. в разделе **Предварительная настройка**) необходимо запустить Web-браузер и перейти на главную страницу iBank 2 UA (стандартный вид страницы представлен на рис. 2.1). Внешний вид главной страницы iBank 2 UA настраивается банком и может отличаться от стандартного.

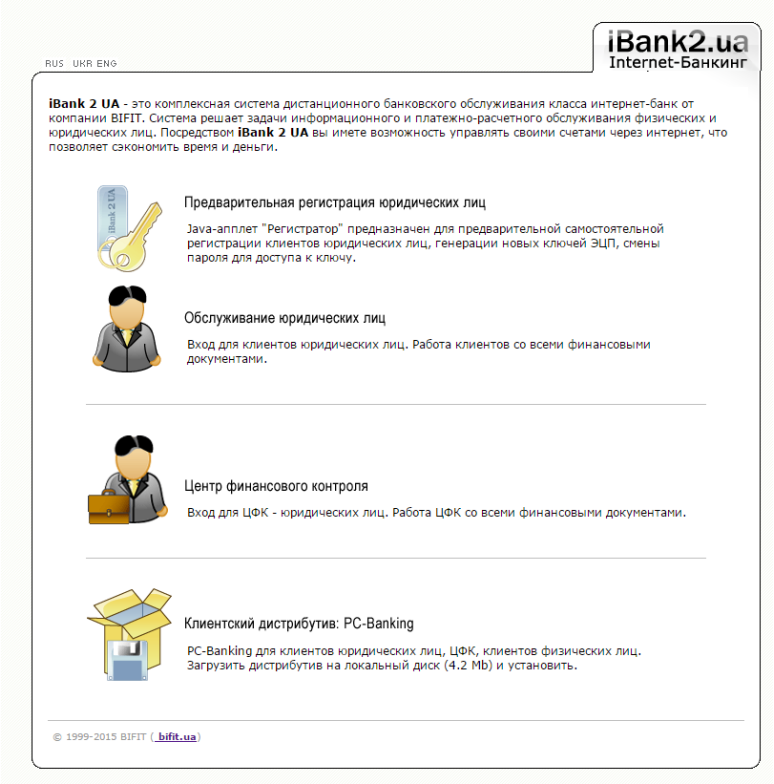


Рис. 2.1. Главная страница системы iBank 2 UA

На главной странице iBank 2 UA необходимо выбрать пункт **Предварительная регистрация юридических лиц**, в результате чего сначала загрузится стартовая html-страница (см. рис. 2.2), а через 15 – 30 секунд (в зависимости от скорости доступа в Интернет) загрузится АРМ **Регистратор**.

Внимание!

АРМ **Регистратор** представляет собой последовательность шагов, которые необходимо выполнить для предварительной регистрации корпоративного клиента, новой пары ключей ЭЦП и т. п. Внешний вид и состав шагов настраиваются банком и могут отличаться от описанных шагов в данном документе.

Рис. 2.2. Стартовая html-страница для загрузки Java-апплета **Регистратор**

В результате на экране появится окно АРМ **Регистратор** на шаге настройки подключения к банковскому серверу с использованием proxy-сервера (см. рис. 2.3). Если для доступа к сети Интернет используется proxy-сервер, то клиенту необходимо включить соответствующую отметку, а также указать адрес и порт proxy-сервера. Если доступ к сети Интернет происходит без использования proxy-сервера, то данный шаг пропускается.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**.

Выбор раздела АРМ

После настройки подключения к банковскому серверу выполняется переход на шаг выбора раздела АРМ (см. рис. 2.4):

1. ***Новый клиент*** — переход к предварительной регистрации корпоративного клиента;
2. ***Новые ключи ЭЦП*** — переход к генерации новой пары ключей ЭЦП;
3. ***Администрирование ключей ЭЦП*** — переход к разделу управления ключами ЭЦП корпоративного клиента.

При нажатии кнопки **Далее** выполняется переход на первый шаг соответствующего раздела.

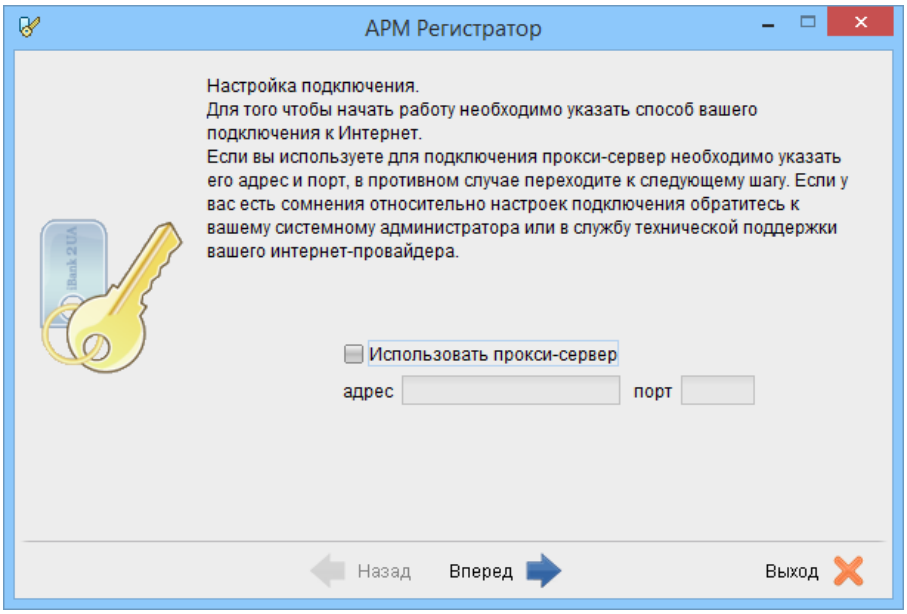


Рис. 2.3. Шаг настройки подключения к банковскому серверу

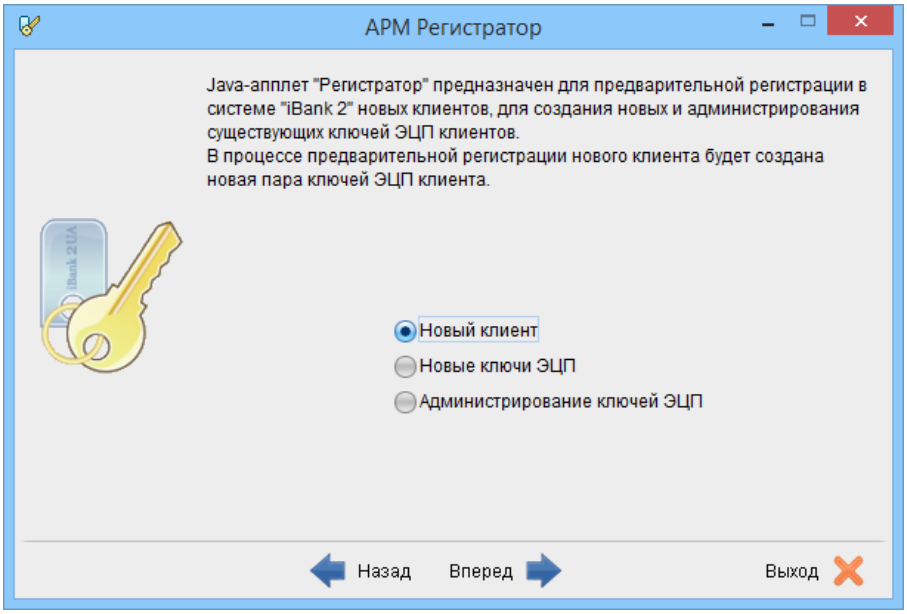


Рис. 2.4. Шаг выбора раздела АРМ **Регистратор**

Раздел 3

Регистрация корпоративного клиента

Предварительная регистрация в АРМ Регистратор

Предварительная регистрация корпоративного клиента заключается в последовательном заполнении ряда экранных форм в АРМ **Регистратор** реквизитами организации и другой информацией, необходимой для заключения договора и дальнейшего обслуживания. Процедура предварительной регистрации при наличии всех необходимых реквизитов организации занимает от 5 до 10 мин.

Ввод реквизитов организации

При выборе варианта **Новый клиент** на шаге выбора раздела АРМ **Регистратор** выполняется переход на шаг ввода реквизитов организации (см. рис. 3.1). На данном шаге необходимо указать основные реквизиты организации: наименование, юридический адрес и код ЕГРПОУ. Реквизиты на английском языке необязательны для заполнения.

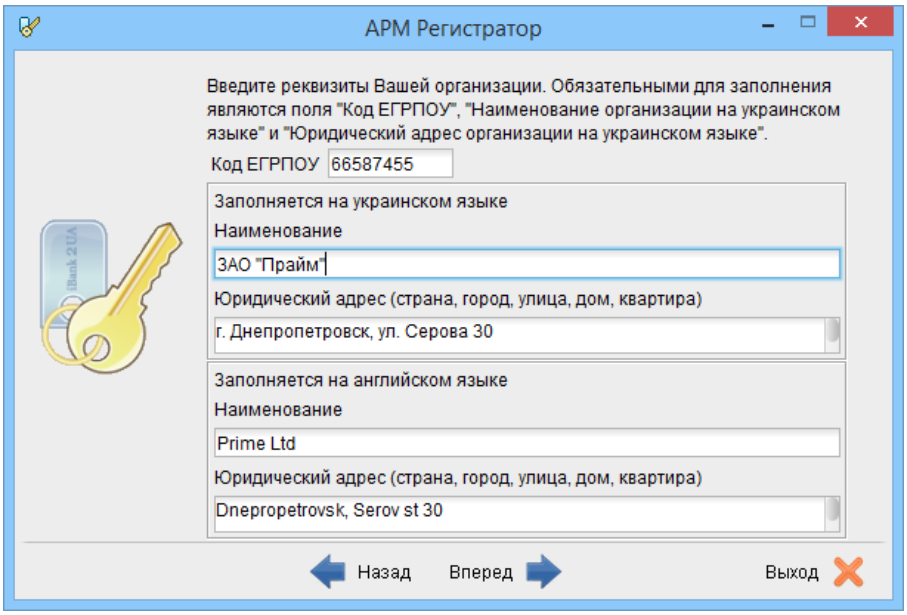


Рис. 3.1. Шаг ввода реквизитов организации

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Кнопка становится доступной только после заполнения обязательных полей.

Добавление счетов организации

После ввода реквизитов организации выполняется переход на шаг добавления счетов организации, с которыми в дальнейшем будет работать клиент (см. рис. 3.2).

Для добавления счета необходимо выполнить следующие действия:

1. Выбрать код МФО банка, в котором открыт счет;
2. Ввести номер счета;

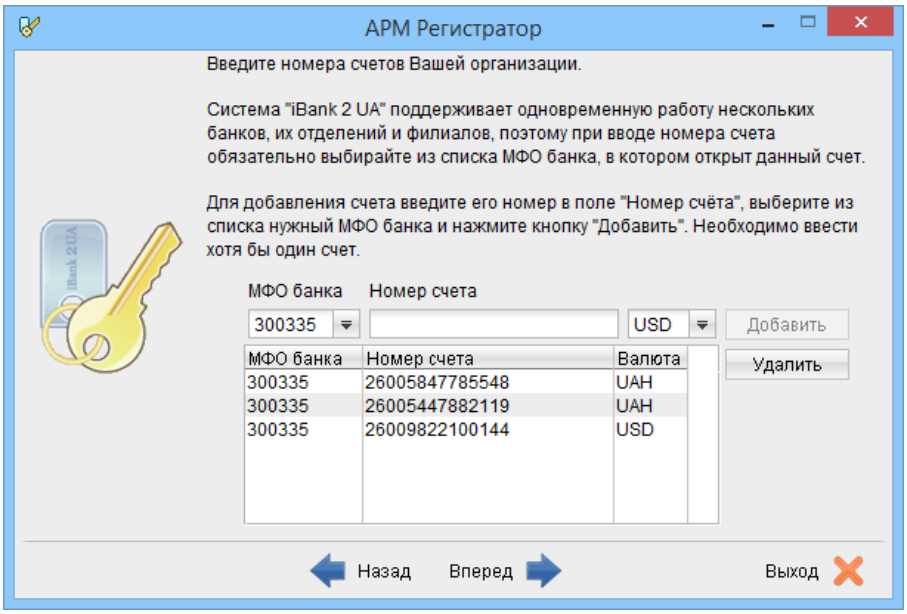


Рис. 3.2. Шаг добавления счетов организации

3. Выбрать валюту счета;

> ***Внимание!***
> Состав списка валют настраивается сотрудником банка. За дополнительной информацией следует обратиться в отдел технической поддержки обслуживающего банка.

4. Нажать кнопку **Добавить**. Если на экран выводится сообщение об ошибке ключевания счета, то это означает, что введен неверный номер счета или номер счета не соответствует коду МФО банка. Если ошибка появляется при верно введенной информации, то необходимо обратиться в отдел технической поддержки обслуживающего банка.

   Аналогичным образом следует добавить другие счета организации.

При необходимости можно удалить счет из списка добавленных счетов. Для этого следует выбрать нужный счет в списке и нажать кнопку **Удалить**.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Кнопка становится доступной только после добавления хотя бы одного счета.

Заполнение информации о контактном лице организации

После добавления счетов организации выполняется переход на шаг заполнения информации о контактном лице организации (см. рис. 3.3). На данном шаге можно заполнить следующую информацию: ФИО, номера телефона и факса, а также e-mail. Факс и e-mail необязательны для заполнения.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Кнопка становится доступной только после заполнения обязательных полей.

Ввод блокировочного слова

После заполнения информации о контактном лице организации выполняется переход на шаг ввода блокировочного слова и выбора количества групп подписей под документами (см. рис. 3.4).

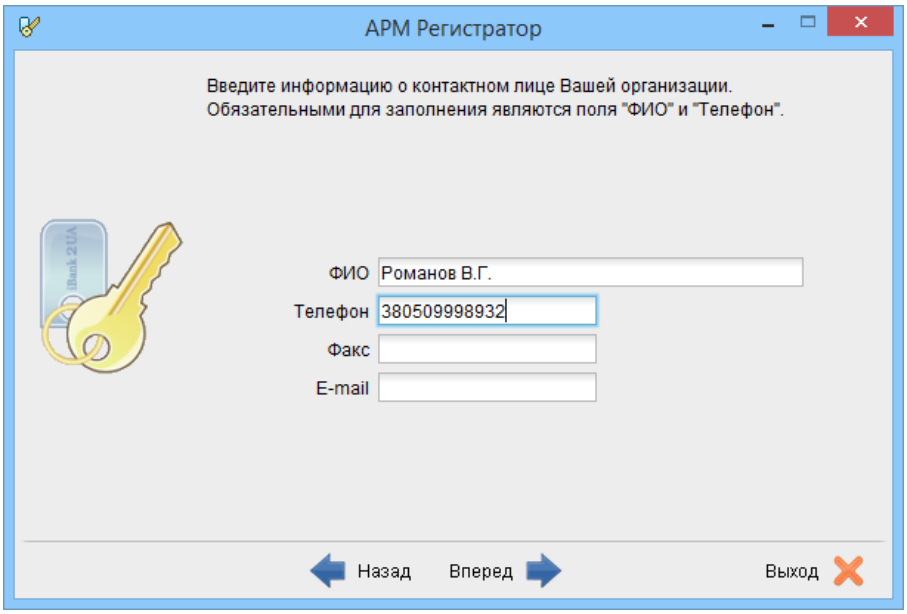


Рис. 3.3. Шаг заполнения информации о контактном лице организации

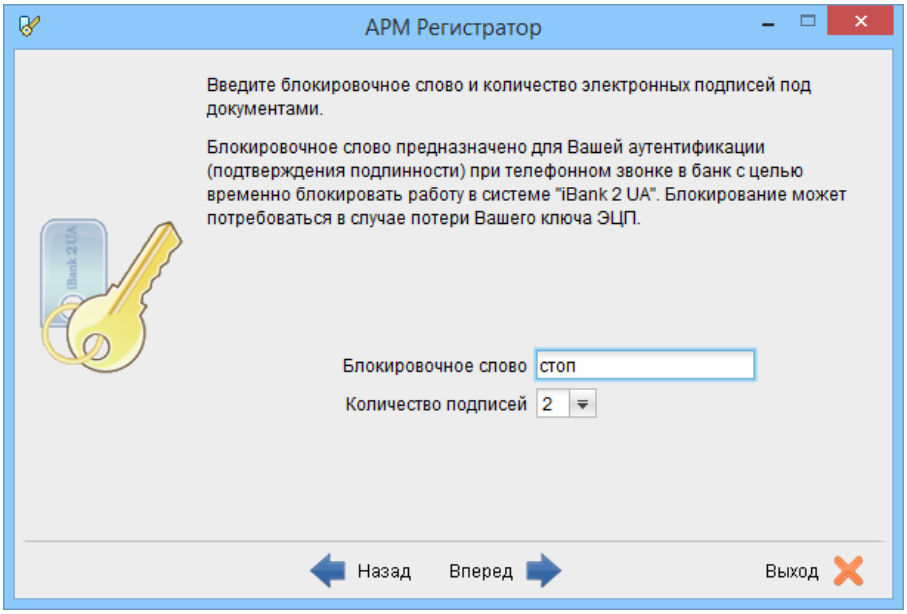


Рис. 3.4. Шаг ввода блокировочного слова

Блокировочное слово необходимо для аутентификации клиента при телефонном звонке в обслуживающий банк с целью временно заблокировать его работу в системе iBank 2 UA (например, при подозрении в компрометации секретного ключа ЭЦП). Блокировочное слово является секретным словом, поэтому клиент не сможет его увидеть при дальнейшей работе в iBank 2 UA.

Количество *электронных подписей* под документами определяет количество *групп электронных подписей*. Электронные подписи, входящие в одну группу, взаимозаменяемы при подписи документов. Например, если генеральный директор и заместитель генерального директора имеют право первой подписи под финансовыми документами, то они будут в одной, первой группе. Соответственно, главный бухгалтер и заместитель главного бухгалтера, имеющие право второй подписи под финансовыми документами, также будут в одной, но уже во второй группе (право

второй подписи). Как правило, клиент выбирает две группы подписи – директора и главного бухгалтера.

Внимание!

При наличии более чем одной группы подписи необходимо сгенерировать дополнительные пары ключей ЭЦП. Дополнительные пары ключей можно сгенерировать как в процессе регистрации нового корпоративного клиента (подробнее см. в подразделе **Печать сертификата открытого ключа ЭЦП**), так и позднее (подробнее см. в подразделе **Создание новых ключей ЭЦП**).

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Кнопка становится доступной только после ввода блокировочного слова.

Проверка введенной информации

После ввода блокировочного слова выполняется переход на шаг проверки введенной ранее информации (см. рис. 3.5).

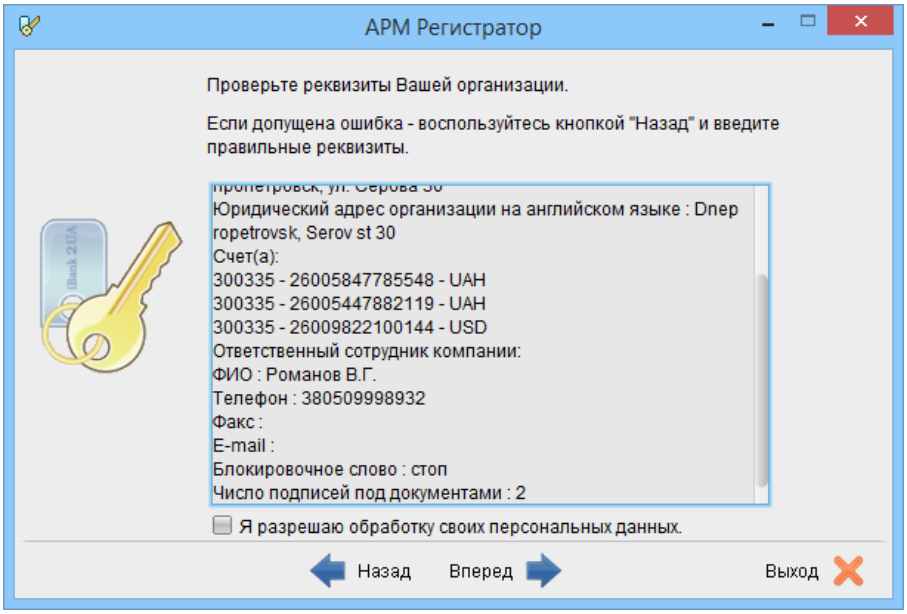


Рис. 3.5. Шаг проверки введенной ранее информации

В случае обнаружения ошибки необходимо последовательными нажатиями кнопки **Назад** вернуться на соответствующий шаг для ее исправления.

Для перехода к следующему шагу необходимо включить отметку разрешения обработки своих персональных данных и нажать кнопку **Далее**.

Регистрация новой пары ключей ЭЦП при регистрации нового клиента

Во время предварительной регистрации корпоративного клиента автоматически генерируется новая пара ключей ЭЦП, которая привязывается сотруднику организации. Таким образом, в результате предварительной регистрации, клиент регистрируется с одним сотрудником, к которому привязан ключ ЭЦП. Для регистрации других сотрудников организации необходимо отдельно сгенерировать новые пары ключей ЭЦП. Дополнительные пары ключей можно сгенерировать как в процессе регистрации нового корпоративного клиента (подробнее см. в подразделе **Печать**

сертификата открытого ключа ЭЦП), так и позднее (подробнее см. в подразделе **Создание новых ключей ЭЦП**).

Ввод информации о владельце ключа

После проверки введенной информации выполняется переход на шаг ввода ФИО и должности сотрудника организации, к которому будет привязан сгенерированный на последующих шагах ключ ЭЦП (см. рис. 3.6). Указанное ФИО также будет сохранено в качестве владельца ключа ЭЦП. Информация о владельце ключа необходима для идентификации сотрудника организации, который выполнял действия над финансовыми документами.

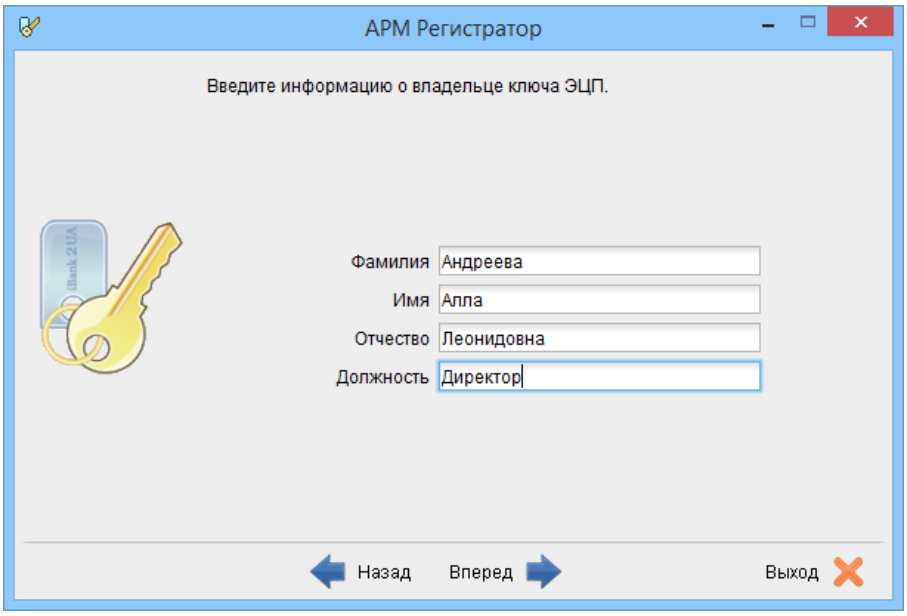


Рис. 3.6. Шаг ввода информации о владельце ключа

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Информация о владельце ключа необязательна для заполнения.

Выбор хранилища ключа ЭЦП

После ввода информации о владельце ключа выполняется переход на шаг выбора хранилища ключа ЭЦП (см. рис. 3.7). В системе iBank 2 UA поддерживаются следующие виды хранилищ ключей:

- ***Файл на диске*** — ключи ЭЦП хранятся в файле на съемном или несъемном носителе;
- ***USB-токен*** — ключи ЭЦП хранятся на USB-токене – устройстве для безопасного хранения ключей ЭЦП, подключаемом к USB порту компьютера. В отличие от других съемных носителей, с USB-токена невозможно скопировать ключи ЭЦП, что существенно снижает возможность несанкционированного доступа к ключу ЭЦП клиента.

  Внимание!
  Для выбора USB-токена из списка хранилища ключей его необходимо подключить в USB-порт компьютера.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. В зависимости от выбранного хранилища ключей ЭЦП следующие три шага будут отличаться.

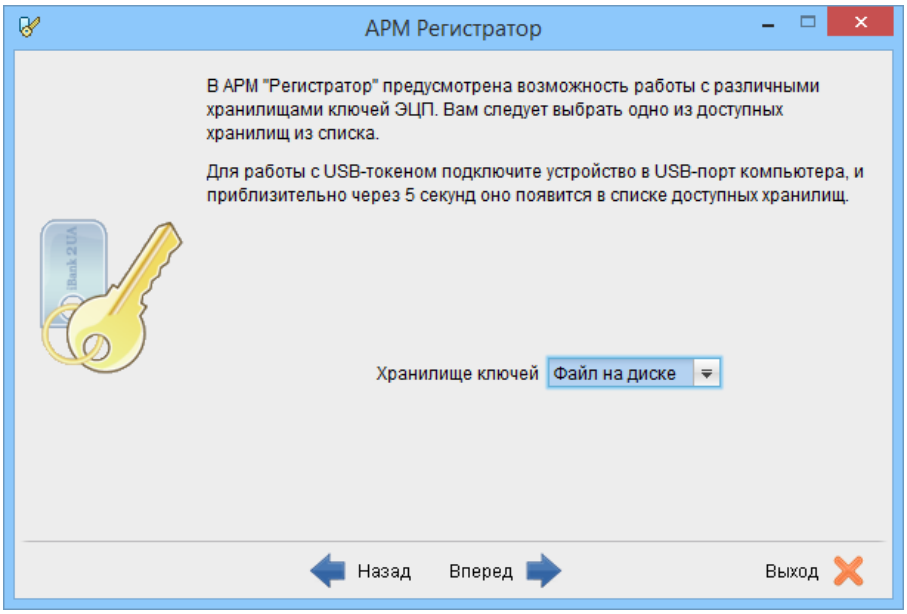


Рис. 3.7. Шаг выбора хранилища ключа ЭЦП

Регистрация новой пары ключей ЭЦП на USB-токене

Первичная установка USB-токена

Если в качестве хранилища ключей ЭЦП был выбран USB-токен, который еще не был инициализирован, то выполняется переход на шаг инициализации USB-токена (см. рис. 3.8). На данном шаге необходимо указать следующую информацию:

- Наименование устройства. Отображается, если USB-токен поддерживает одновременное хранение нескольких активных ключей ЭЦП. Указанное наименование устройства будет отображаться клиенту в дальнейшей работе (например, при выборе хранилища ключа в окне **Вход в систему** АРМ **Internet-Банкинг для корпоративных клиентов** (описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Internet-Банкинг для корпоративных клиентов. Руководство пользователя***)).
- Пароль на устройство. Минимальная длина составляет 6 символов.
- Код разблокировки. Отображается, если устройство поддерживает возможность разблокирования. Минимальная длина составляет 8 символов.

При вводе пароля и кода разблокировки учитывается текущая раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями для ввода кода разблокировки (или пароля, если устройство не поддерживает возможность разблокирования) отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

Для перехода к следующему шагу необходимо заполнить все поля и нажать кнопку **Далее**.

Ввод пароля на USB-токен

Если в качестве хранилища ключей ЭЦП был выбран USB-токен, который был инициализирован, то выполняется переход на шаг ввода пароля к устройству (см. рис. 3.9).

При вводе пароля учитываются текущая раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или прописные буквы). После поля ввода пароля отображается

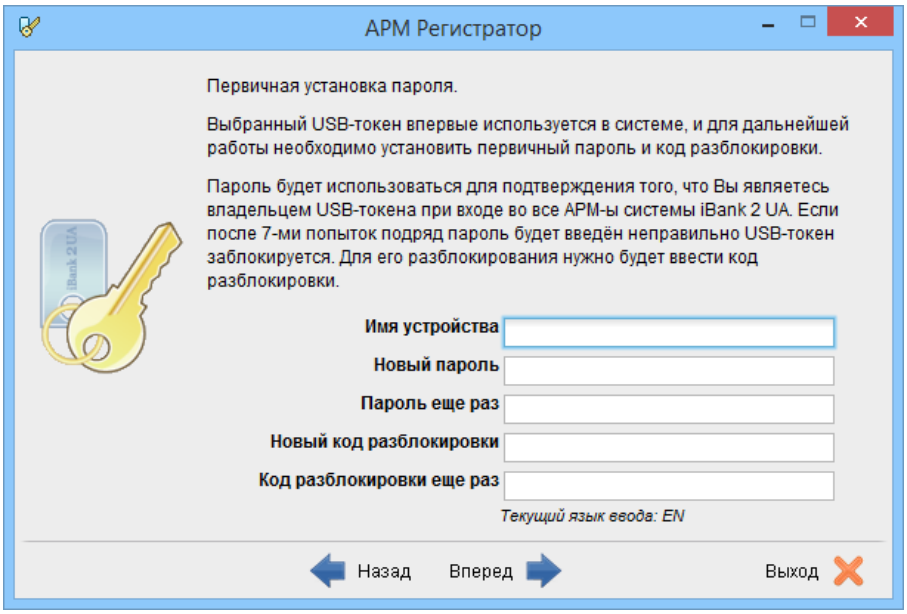


Рис. 3.8. Шаг первичной инициализации USB-токена

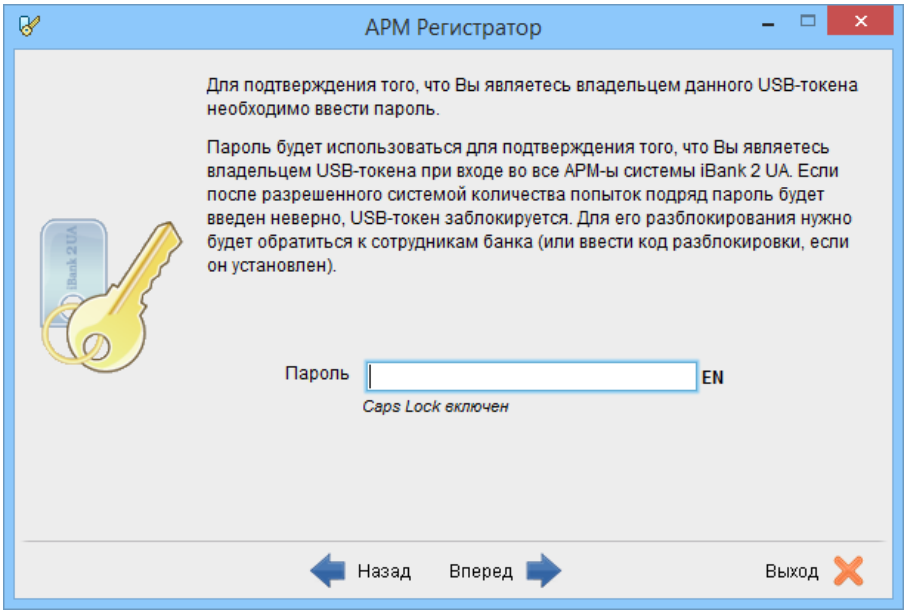


Рис. 3.9. Шаг ввода пароля на USB-токен

подсказка о текущей раскладке клавиатуры. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

При вводе неверного пароля несколько[1] раз подряд устройство будет заблокировано. Если устройство поддерживает возможность разблокирования, то будет выполнен переход на шаг разблокирования устройства (подробнее см. в подразделе **Разблокирование USB-токена**). Если возможность разблокирования устройства не поддерживается, то необходимо обратиться в отдел технической поддержки обслуживающего банка.

Для перехода к следующему шагу необходимо ввести пароль и нажать кнопку **Далее**.

[1] Количество попыток ввода неверного пароля зависит от типа устройства.

Разблокирование USB-токена

Если в качестве хранилища ключа ЭЦП был выбран USB-токен, который заблокирован и для которого поддерживается разблокирование, то выполняется переход на шаг разблокирования устройства (см. рис. 3.10).

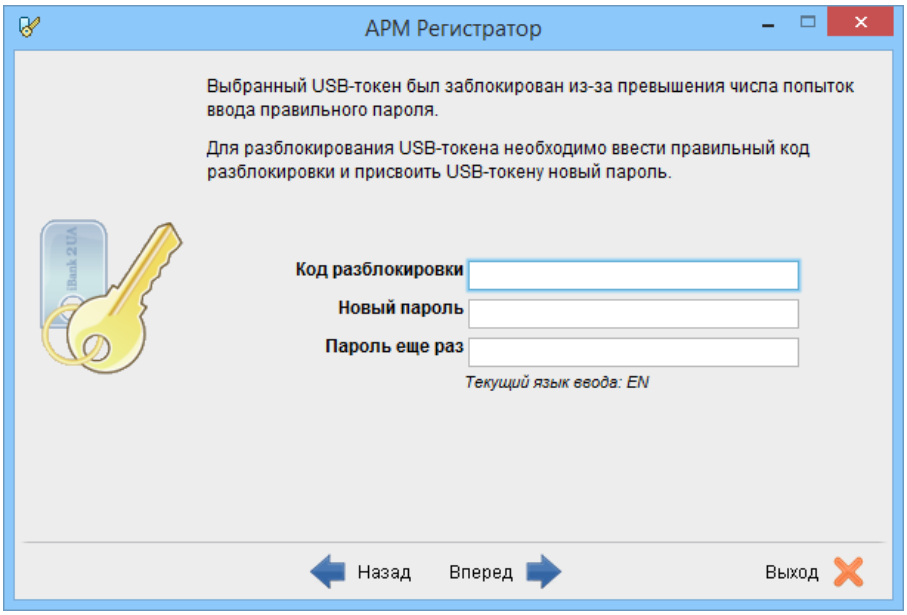


Рис. 3.10. Шаг разблокирования USB-токена

Для разблокирования устройства необходимо ввести код разблокировки, а также установить новый пароль на устройство. При вводе учитываются раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями ввода пароля отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

При вводе неверного кода разблокирования несколько[2] раз подряд устройство будет окончательно заблокировано. Для получения дальнейших инструкций необходимо обратиться в отдел технической поддержки обслуживающего банка.

Для перехода к следующему шагу необходимо заполнить все поля и нажать кнопку **Далее**.

Ввод наименования ключа

После первичной инициализации, ввода пароля к устройству или его разблокирования, выполняется переход на шаг ввода наименования ключа ЭЦП (см. рис. 3.11).

Если устройство не поддерживает одновременное хранение нескольких активных ключей ЭЦП, то указанное наименование ключа будет являться наименованием устройства.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. При этом будет сгенерирована новая пара ключей ЭЦП.

Тестирование новой пары ключей ЭЦП на USB-токене

После генерации новой пары ключей ЭЦП выполняется переход на шаг тестирования сгенерированных ключей (см. рис. 3.12). В ходе тестирования проверяется правильность записи секретного ключа ЭЦП клиента на устройство и корректность регистрации открытого ключа ЭЦП клиента в банке.

[2]Количество попыток ввода неверного кода разблокировки зависит от типа устройства.

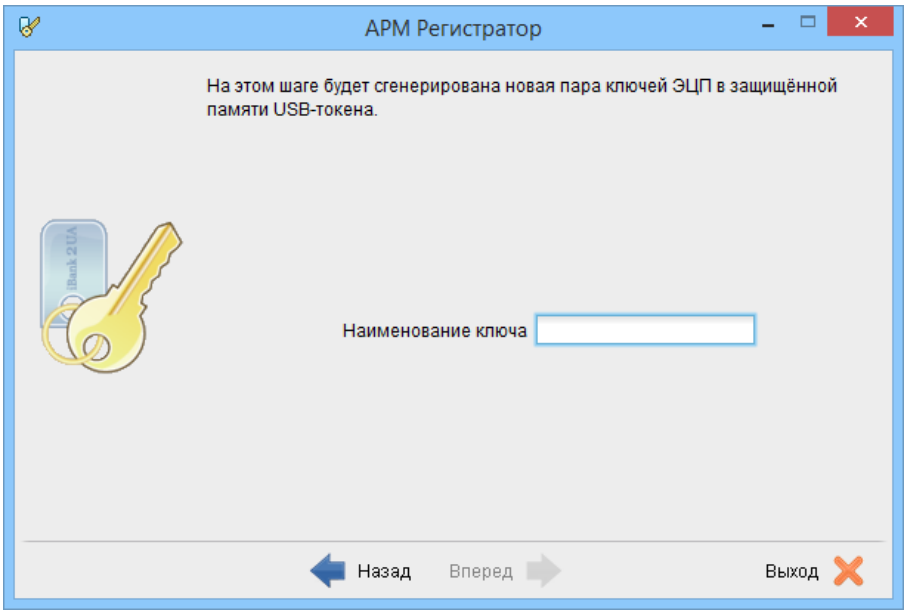


Рис. 3.11. Шаг ввода наименования ключа ЭЦП

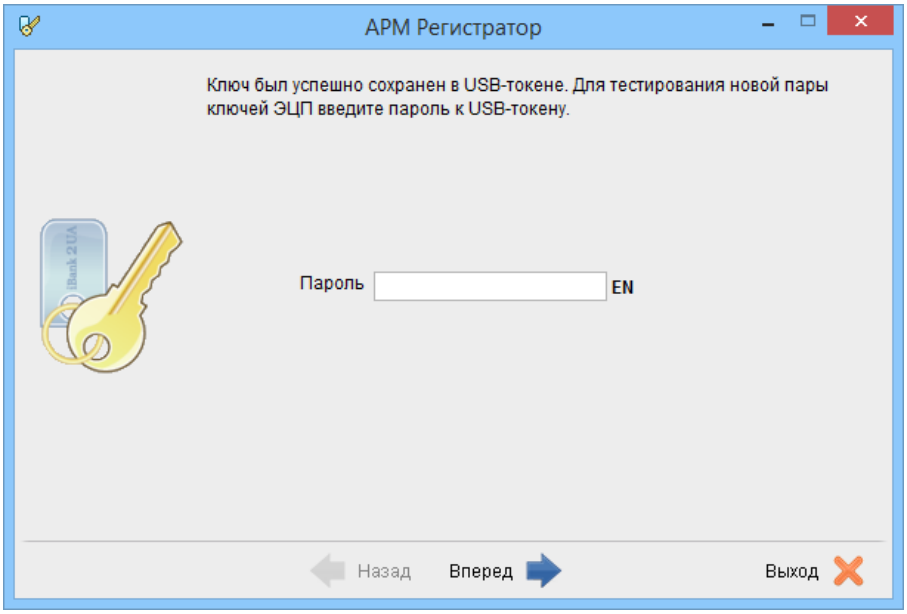


Рис. 3.12. Шаг тестирования ключа на USB-токене

Для тестирования ключа необходимо ввести пароль к устройству. При вводе учитываются раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). После поля ввода пароля отображается подсказка о текущей раскладке клавиатуры. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

При вводе неверного пароля несколько[3] раз подряд устройство будет заблокировано. Если устройство поддерживает возможность разблокирования, то будет выполнен переход на шаг разблокирования устройства (подробнее см. в подразделе **Разблокирование USB-токена**). После разблокирования устройства будет выполнен возврат на шаг тестирования новой пары ключей

[3] Количество попыток ввода неверного пароля зависит от типа устройства.

ЭЦП. Если возможность разблокирования устройства не поддерживается, то необходимо обратиться в отдел технической поддержки обслуживающего банка.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. При этом выполняется переход на шаг печати сертификата открытого ключа ЭЦП (подробнее см. в подразделе **Печать сертификата открытого ключа ЭЦП**).

Регистрация новой пары ключей ЭЦП в файле

Выбор файла хранилища ключа ЭЦП

Если в качестве хранилища ключа ЭЦП был выбран файл на диске, то выполняется переход на шаг выбора файла, который будет использоваться в качестве хранилища ключа (см. рис. 3.13). В одном файле могут храниться несколько ключей ЭЦП одного или разных клиентов.

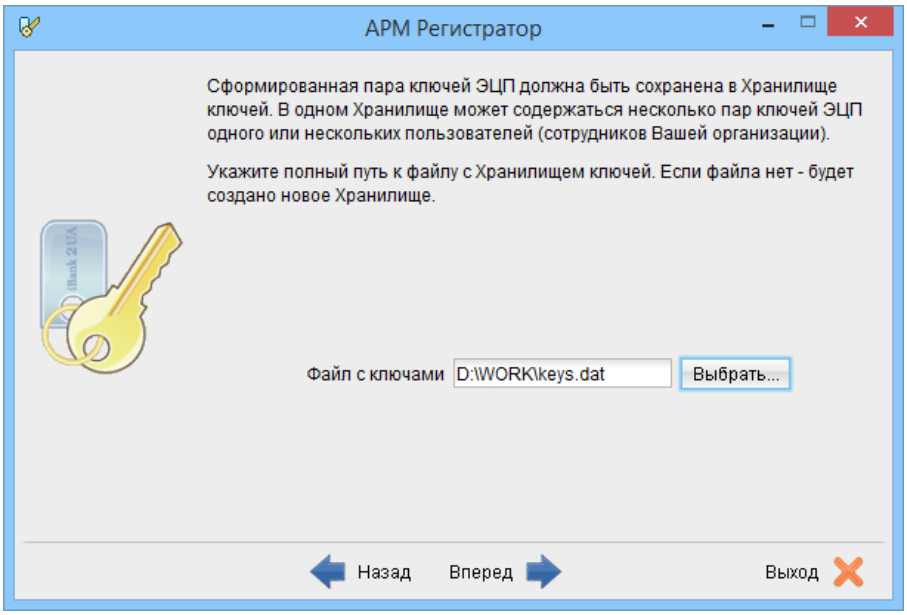


Рис. 3.13. Шаг выбора файла хранилища ключа ЭЦП

Для выбора файла хранилища ключа ЭЦП можно воспользоваться двумя способами:

- Ввести вручную путь к файлу хранилища ключа ЭЦП.
- Нажать кнопку **Выбрать...**, в результате чего на экране откроется стандартный диалог выбора файла. Если при выборе файла был указан только каталог, то в качестве хранилища ключа ЭЦП будет использоваться файл **keys.dat** в выбранном каталоге.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. Если выбранного файла не существует, то система его создаст.

Ввод наименования и пароля ключа ЭЦП в файле

После выбора нужного файла выполняется переход на шаг ввода наименования и пароля ключа ЭЦП, который будет сгенерирован (см. рис. 3.14).

Наименование ключа можно указать двумя способами:

- Ввести вручную;

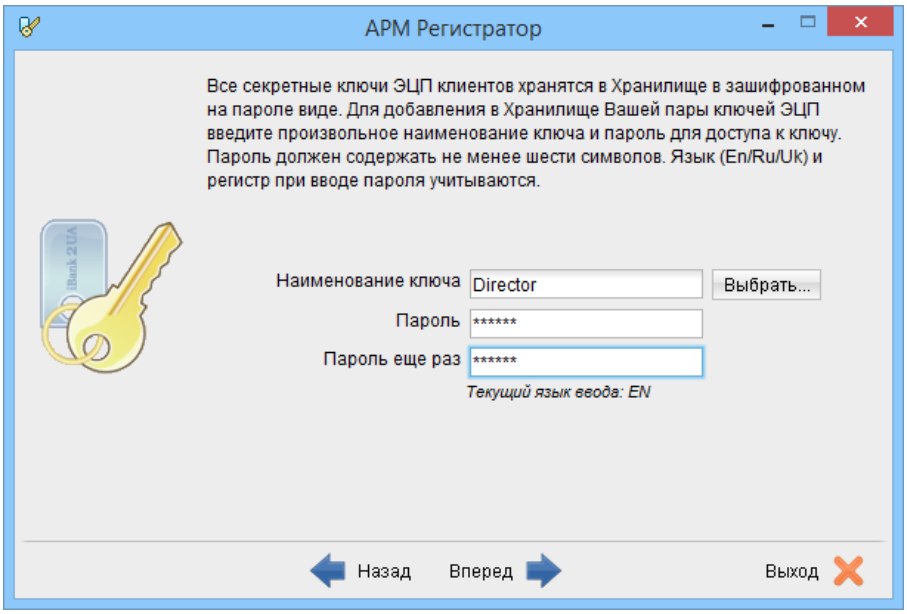


Рис. 3.14. Шаг ввода наименования и пароля ключа ЭЦП в файле

- Выбрать ключ из списка ключей, которые содержатся в файле. Для этого необходимо нажать кнопку **Выбрать...**, в результате чего на экране откроется окно со списком ключей ЭЦП, которые содержатся в файле (см. рис. 3.15).

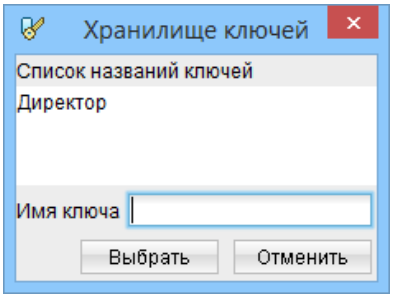


Рис. 3.15. Список ключей ЭЦП, которые содержатся в файле

Внимание!

Если наименование ключа ЭЦП совпадает с другим ключом из файла, то ранее записанный под таким именем ключ будет заменен.

Указанное наименование ключа будет отображаться клиенту в дальнейшей работе (например, при выборе ключа ЭЦП в окне **Вход в систему** АРМ **Internet-Банкинг для корпоративных клиентов** (описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Internet-Банкинг для корпоративных клиентов. Руководство пользователя***)).

Для установки пароля на ключ ЭЦП необходимо в соответствующие поля ввести нужное значение. Минимальная длина пароля 6 символов. При вводе пароля учитываются раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями для ввода пароля отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**. При этом будет сгенерирована новая пара ключей ЭЦП.

Тестирование новой пары ключей ЭЦП

После генерации новой пары ключей ЭЦП выполняется переход на шаг тестирования сгенерированных ключей (см. рис. 3.16). В ходе тестирования проверяется правильность записи секретного ключа ЭЦП клиента в файл хранилища ключа и корректность регистрации открытого ключа ЭЦП клиента в банке.

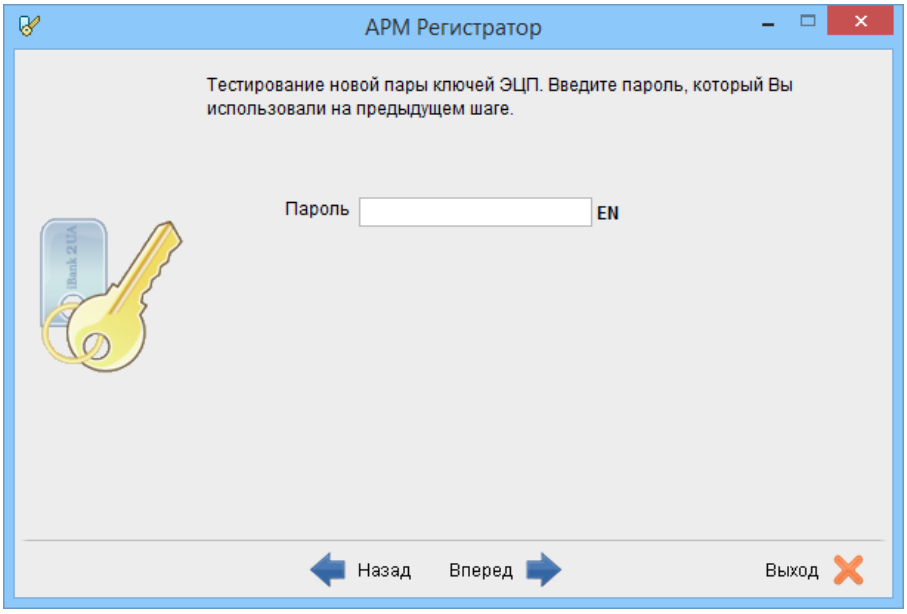


Рис. 3.16. Шаг тестирования новой пары ключей ЭЦП

Для тестирования ключа необходимо ввести пароль, указанный на предыдущем шаге. После поля ввода пароля отображается подсказка о текущей раскладке клавиатуры. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**.

Печать сертификата открытого ключа ЭЦП

Если тестирование новой пары ключей ЭЦП прошло успешно, то выполняется переход на шаг, в котором отображается следующая информация (см. рис. 3.17):

- Идентификатор открытого ключа ЭЦП.
- Отметка **Распечатать сертификат**. Клиент может распечатать сертификат на принтер или в RTF-файл.

> ***Внимание!***
> Вместе с сертификатом открытого ключа ЭЦП также может быть выведен на печать документ о предоставлении прав на счета и документы сотрудника корпоративного клиента. Возможность печати данного документа настраивается сотрудником банка.
> За дополнительной информацией необходимо обратиться в отдел технической поддержки обслуживающего банка.

- Отметка **Создать еще одну пару ключей ЭЦП**. Данная возможность позволяет проводить регистрацию дополнительных ключей ЭЦП без перезапуска АРМ **Регистратор**.

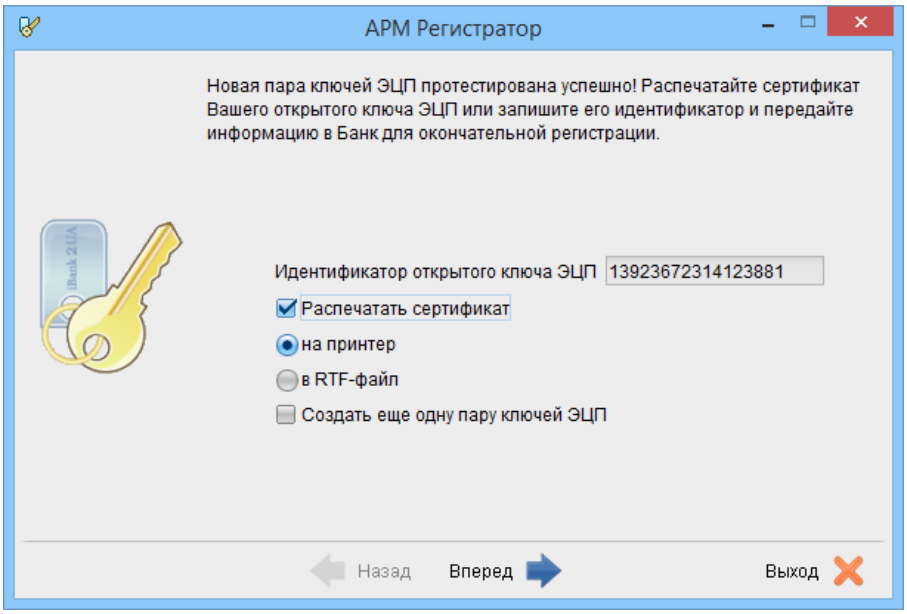


Рис. 3.17. Шаг печати сертификата открытого ключа ЭЦП

При нажатии кнопки **Далее** в зависимости от включенных отметок будут выполняться следующие действия:

1. Если включена отметка **Распечатать сертификат**, то осуществляется вывод сертификата открытого ключа ЭЦП на печать.

2. После печати сертификата или если отметка **Распечатать сертификат** выключена:

   - Если включена отметка **Создать еще одну пару ключей ЭЦП**, то выполняется переход на шаг ввода информации о владельце ключа (подробнее см. в подразделе **Ввод информации о владельце ключа**).
   - Если выключена отметка **Создать еще одну пару ключей ЭЦП**, то выполняется переход на финальный шаг регистрации (см. рис. 3.18). В данном окне описаны дальнейшие инструкции клиента для окончательной регистрации в системе iBank 2 UA.

На этом процесс предварительной регистрации клиента в АРМ **Регистратор** завершается, при этом клиент приобретает в системе iBank 2 UA статус Новый. Для окончательной регистрации клиенту необходимо лично явиться в офис банка (подробнее см. в подразделе **Окончательная регистрация клиента в отделении банка**).

Внимание!
Информация о вновь зарегистрированном клиенте хранится в системе в течении срока, определенного банком (по умолчанию 30 дней). Если к моменту окончания этого срока клиент не прошел окончательную регистрацию в офисе банка, то информация о клиенте удаляется с банковского сервера.

Окончательная регистрация клиента в отделении банка

Для окончательной регистрации клиенту необходимо лично явиться в отделение банка. При себе клиенту следует иметь распечатанный сертификат открытого ключа ЭЦП (или записанный идентификатор открытого ключа), документ об удостоверении личности, а также другие документы, требуемые банком при заключении договора с клиентом.

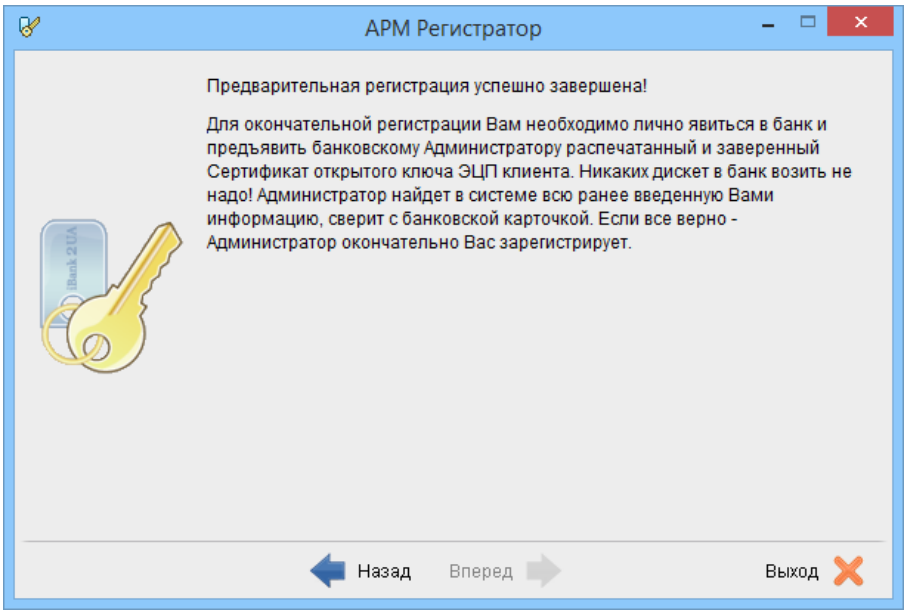


Рис. 3.18. Финальный шаг регистрации

После предъявления клиентом сертификата или идентификатора открытого ключа ЭЦП сотрудник банка выполнит следующие действия:

1. По идентификатору открытого ключа ЭЦП найдет в системе информацию о клиенте, проверит и в случае необходимости откорректирует ее;
2. Распечатает и предоставит клиенту на подпись договор на обслуживание клиента в системе iBank 2 UA;
3. Установит клиенту права на работу с определенными типами документов и отчетов, а также права на работу в различных модулях системы iBank 2 UA;
4. Активирует ключи ЭЦП клиента. Если клиент заранее создал дополнительные ключи в АРМ **Регистратор** (подробнее см. в разделе **Создание новых ключей ЭЦП**), то сотрудник банка активирует все необходимые ключи и определит для них группу подписи в соответствии с требованием клиента.
5. Окончательно зарегистрирует клиента в системе. При этом клиент приобретет статус **Зарегистрированный**.

После завершения регистрации в отделении банка и подписания договора на обслуживание, клиент может работать в системе iBank 2 UA. Основная работа корпоративного клиента в системе проходит в АРМ **Internet-Банкинг для корпоративных клиентов** (подробное описание представлено в документации ***Система iBank 2 UA. Internet-Банкинг для корпоративных клиентов. Руководство пользователя***), **PC-Банкинг для корпоративных клиентов** (подробное описание представлено в документации ***Система iBank 2 UA. PC-Банкинг для корпоративных клиентов. Руководство пользователя***) или **Web-Банкинг для корпоративных клиентов** (подробное описание представлено в документации ***Система iBank 2 UA. Web-Банкинг для корпоративных клиентов. Руководство пользователя***).

Регистрация управляющего клиента (ЦФК)

В системе iBank 2 UA реализована специальная схема обслуживания крупных корпоративных клиентов с территориально удаленными подразделениями, филиалами и дочерними структурами под названием **Центр Финансового Контроля** (далее - ЦФК). ЦФК представляет собой абстрактного клиента (управляющая организация) системы iBank 2 UA, к которому привязываются зарегистрированные корпоративные клиенты (подчиненные клиенты).

Для регистрации ЦФК в системе необходимо выполнить следующие действия:

1. Зарегистрировать подчиненных клиентов в качестве корпоративных клиентов системы iBank 2 UA (подробнее см. в разделе **Регистрация корпоративного клиента**).

2. Для регистрации управляющего клиента (ЦФК) **не нужно** регистрировать нового корпоративного клиента. Вместо этого необходимо сгенерировать новую пару ключей ЭЦП (подробнее см. в разделе **Регистрация ключей ЭЦП**). Если от имени управляющего клиента в системе iBank 2 UA будут работать несколько сотрудников, то необходимо сгенерировать новую пару ключей ЭЦП для каждого из них.

3. Для работы ЦФК с финансовыми документами подчиненных клиентов необходимо каждому из них зарегистрировать «виртуальных» сотрудников. При работе ключи ЭЦП «виртуальных» сотрудников должны находиться в одном каталоге с ключами ЭЦП сотрудника управляющей организации.

При окончательной регистрации управляющего клиента в отделении банка необходимо предоставить сертификаты сгенерированных ключей ЭЦП сотрудников управляющей организации и «виртуальных» сотрудников подчиненных клиентов, а также другие документы, запрашиваемые банком. После этого сотрудник банка проверит документы, зарегистрирует управляющего клиента, назначит ему подчиненных клиентов и активирует ключи ЭЦП.

После завершения регистрации в отделении банка, управляющий клиент может работать в системе iBank 2 UA. Работа ЦФК возможна в АРМ **Internet-Банкинг ЦФК** (подробное описание представлено в документации ***Система iBank 2 UA. Internet-Банкинг для Центров финансового контроля. Руководство пользователя***) и **PC-Банкинг ЦФК** (подробное описание представлено в документации ***Система iBank 2 UA. PC-Банкинг для Центров финансового контроля. Руководство пользователя***).

Раздел 4

Регистрация ключей ЭЦП

Создание новых ключей ЭЦП

Процедура генерации новых ключей ЭЦП может быть необходима в следующих случаях:

1. Клиенту, прошедшему предварительную регистрацию, необходимо для работы две пары ключей и более. Например, одна пара ключей ЭЦП с правом первой подписи необходима директору, а вторая пара ключей ЭЦП с правом второй подписи необходима главному бухгалтеру.

2. Зарегистрированный в системе клиент меняет распределение прав подписи финансовых документов (или меняется состав сотрудников, имеющих право подписи финансовых документов). Например, меняется главный бухгалтер, обладающий правом второй подписи, или появляется заместитель директора, обладающий правом первой подписи.

3. Носитель информации с хранилищем ключей был утерян или поврежден.

> ***Внимание!***
> Для быстрой генерации новой пары ключей ЭЦП с идентичными настройками текущего ключа (например, в случае окончания срока действия ключа) корпоративный клиент или ЦФК могут воспользоваться сервисом «Дистанционная смена ключа». Возможность работы клиента с данным сервисом настраивается сотрудником банка. За дополнительной информацией следует связаться с отделом технической поддержки обслуживающего банка.

Сгенерированные ключи ЭЦП могут быть добавлены как уже зарегистрированным сотрудникам организации, так и в качестве ключей новых сотрудников.

Процедура создания новой пары ключей ЭЦП заключается в последовательном заполнении ряда экранных форм в АРМ **Регистратор**. Для перехода к созданию ключей необходимо выбрать пункт **Новые ключи ЭЦП** на шаге выбора раздела АРМ (подробнее см. в разделе **Вход в систему**).

В результате будет выполнен переход на шаг ввода информации о владельце ключа ЭЦП (см. рис. 4.1).

На данном шаге необходимо указать ФИО и должность сотрудника организации, который будет являться владельцем ключа, а также включить отметку о разрешении обработки своих персональных данных. Включение отметки не обязательно, если информация о владельце ключа не указана.

Для перехода к следующему шагу необходимо нажать кнопку **Далее**.

В результате клиент переходит на шаг выбора типа хранилища ключа ЭЦП. Данный шаг и все последующие шаги аналогичны соответствующим шагам при регистрации нового корпоративного клиента (подробнее см. в подразделе **Выбор хранилища ключа ЭЦП**).

> ***Внимание!***
> Предварительно зарегистрированный открытый ключ ЭЦП клиента хранится в системе в течении срока, определенного банком (по умолчанию 30 дней). Если к моменту окончания этого срока ключ ЭЦП не прошел окончательную регистрацию в офисе банка, то информация о ключе удаляется с банковского сервера.

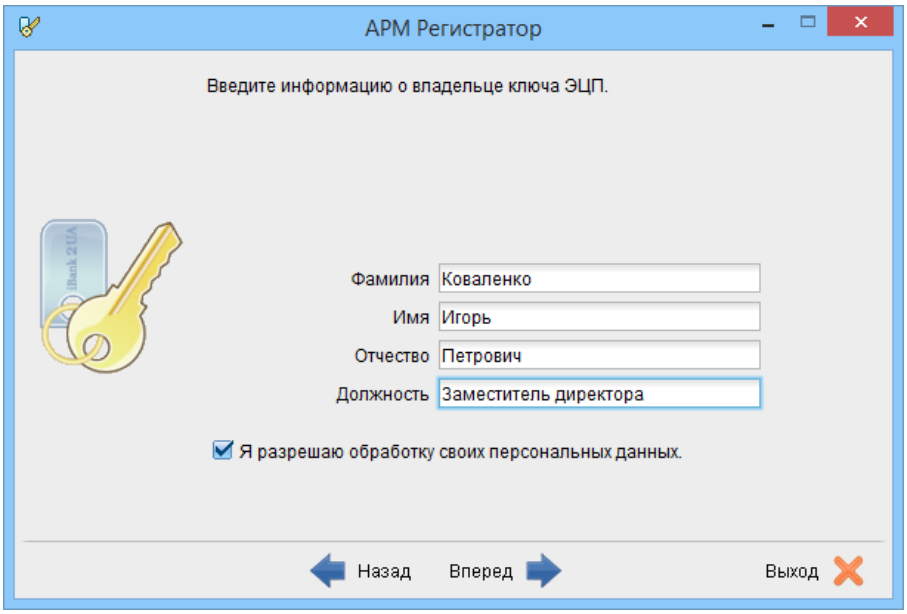


Рис. 4.1. Шаг ввода информации о владельце ключа

Окончательная регистрация новой пары ключей ЭЦП

Для окончательной регистрации новой пары ключей ЭЦП клиенту необходимо лично явиться в отделение банка. При себе следует иметь следующие документы:

- Распечатанный сертификат открытого ключа ЭЦП или записанный идентификатор открытого ключа ЭЦП;
- Документ об удостоверении личности клиента.

Сотрудник банка при предъявлении клиентом документов находит в системе информацию об открытом ключе ЭЦП клиента, сверяет ее с информацией в сертификате (или проверяет совпадение идентификатора, предъявленного клиентом и зарегистрированного в системе). Если не будет обнаружено ошибок, то сотрудник банка зарегистрирует в системе и активирует новую пару ключей ЭЦП, а также установит для нее группу подписи в соответствии с требованием клиента.

Раздел 5

Администрирование ключей ЭЦП

Для перехода в раздел администрирования ключей ЭЦП необходимо выбрать пункт **Администрирование ключей ЭЦП** на шаге выбора раздела АРМ (подробнее см. в разделе **Вход в систему**). В результате будет выполнен переход на шаг выбора типа хранилища ключа ЭЦП. Данный шаг аналогичен соответствующему шагу при регистрации нового клиента (подробнее см. в подразделе **Выбор хранилища ключа ЭЦП**).

В зависимости от выбранного хранилища ключа выполняются следующие действия:

- Если в качестве хранилища ключа выбран USB-токен:

  1. Если устройство было заблокировано и поддерживается его разблокирование, то выполняется переход на шаг разблокирования устройства. Внешний вид данного шага аналогичен соответствующему шагу при регистрации нового клиента (подробнее см. в подразделе **Разблокирование USB-токена**). При попытке выбрать в качестве хранилища ключей ЭЦП USB-токен, который был окончательно заблокирован или еще не был инициализирован, на экране появится соответствующая ошибка.
  2. Если выбрано активное устройство (или после его разблокирования), то выполняется переход на шаг ввода пароля к устройству. Внешний вид данного шага аналогичен соответствующему шагу при регистрации нового клиента (подробнее см. в подразделе **Ввод пароля на USB-токен**).
  3. После ввода пароля к устройству выполняется переход на шаг администрирования ключей ЭЦП на USB-токене (см. рис. 5.1).

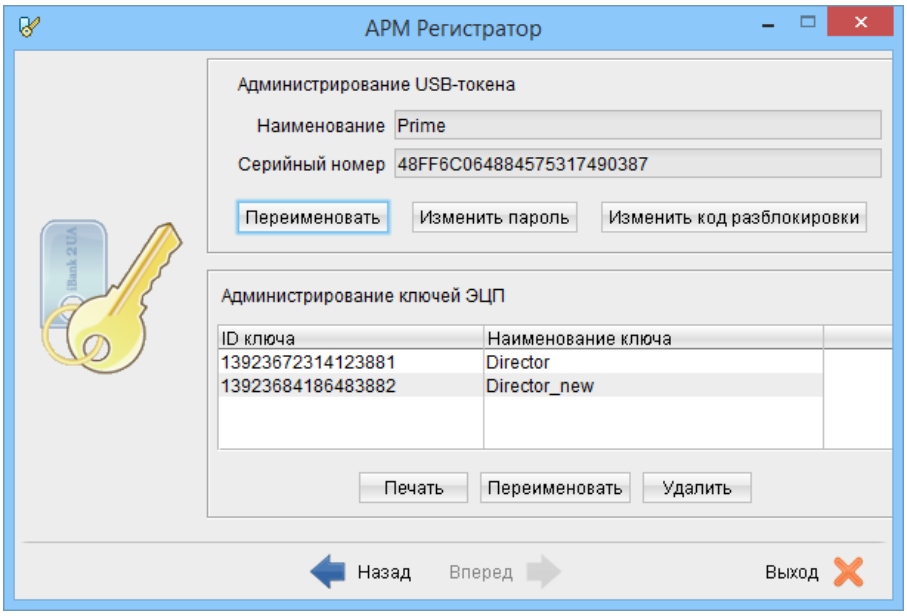


Рис. 5.1. Шаг администрирования ключей ЭЦП на USB-токене

- Если в качестве хранилища ключа выбран файл на диске, то будет выполнен переход на шаг администрирования ключа ЭЦП в файле (см. рис. 5.2). Информация в данном окне представляет собой два списка ключей ЭЦП, которые содержатся в выбранных файлах. Для выбора файла хранилища ключа ЭЦП необходимо нажать кнопку **Выбрать** над соответствующим списком и в появившемся диалоге указать нужный файл.

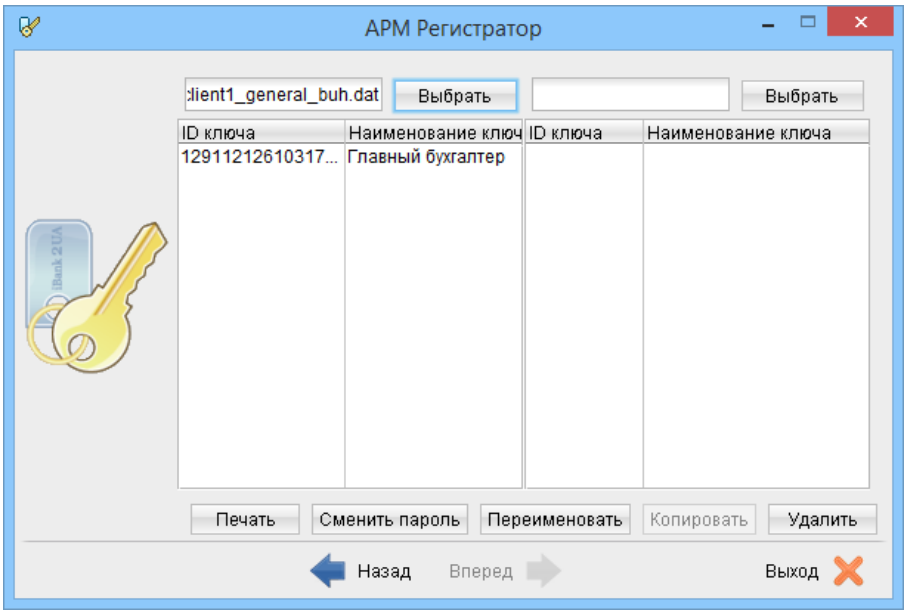


Рис. 5.2. Шаг администрирования ключей ЭЦП в файле

В АРМ **Регистратор** клиенту доступны следующие операции над ключами ЭЦП:

Вывод на печать сертификата — для вывода на печать сертификата ключа ЭЦП необходимо выделить его в списке и нажать кнопку **Печать**.

Если ключ ЭЦП находится в файле, то на экране дополнительно откроется окно **Печать ключа ЭЦП** (см. рис. 5.3) для ввода пароля на ключ. При вводе пароля учитывается раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). После поля ввода пароля отображается подсказка о текущей раскладке. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

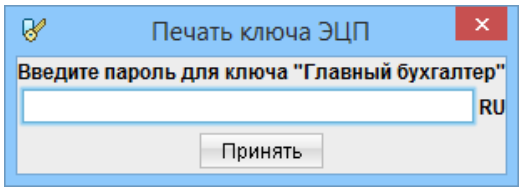
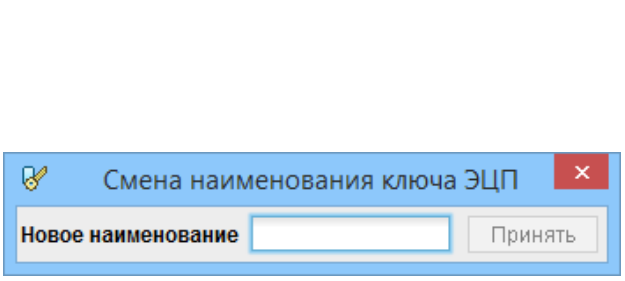


Рис. 5.3. Окно **Печать ключа ЭЦП**

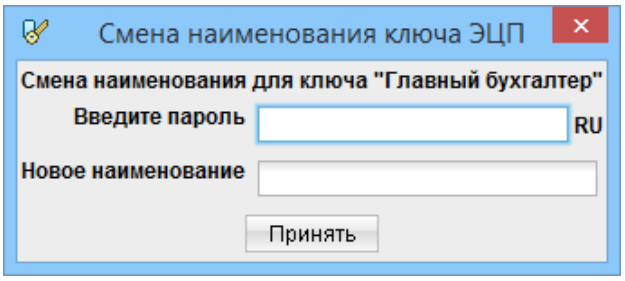
Изменение наименования — доступно для ключей, которые хранятся в файле или на USB-токене, который поддерживает хранение нескольких активных ключей. Для изменения наименования ключа ЭЦП необходимо выделить его в списке и нажать **Переименовать**. В результате откроется окно **Смена наименования ключа ЭЦП** (см. рис. 5.4). При администрировании ключей в файле в окне также необходимо ввести пароль на ключ (см. рис. 5.4(б)).

Удаление — доступно для ключей, которые хранятся в файле или на USB-токене, который поддерживает хранение нескольких активных ключей. Для удаления ключа ЭЦП необходимо выделить его в списке и нажать кнопку **Удалить**.

Если ключ находится в файле, то на экране появится окно **Удаление ключа ЭЦП** (см. рис. 5.5) для ввода пароля на ключ. При вводе пароля учитывается раскладка клавиатуры



а) Ключ на USB-токене



б) Ключ в файле на диске

Рис. 5.4. Окно **Смена наименования ключа ЭЦП**

(украинская, русская, латинская) и регистр (заглавные или строчные буквы). После поля ввода пароля отображается подсказка о текущей раскладке. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

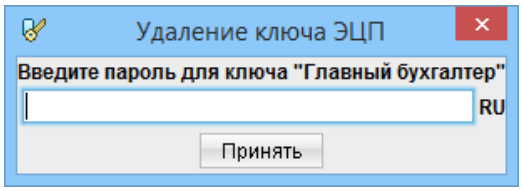


Рис. 5.5. Окно **Удаление ключа ЭЦП**

Внимание!

Если секретный ключ ЭЦП был удален из хранилища ключей, то восстановить его невозможно. Поэтому удалять можно только ключи, которые в дальнейшем не будут использоваться при работе с системой (ключи с истекшим сроком действия, скомпрометированные ключи и т. п.).

Смена пароля — доступно только при администрировании ключей в файле. Для смены пароля на ключ необходимо выделить его в списке и нажать кнопку **Сменить пароль**. В результате на экране откроется окно **Смена пароля** (см. рис. 5.6), в котором необходимо ввести текущий и новый пароли. При вводе пароля учитывается раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

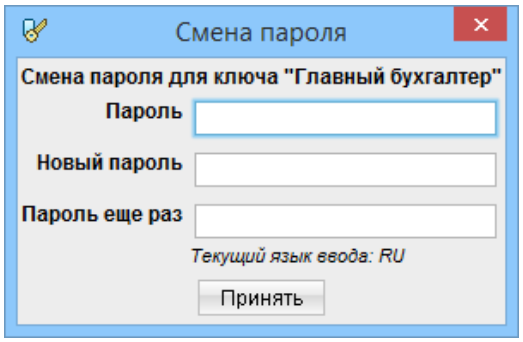


Рис. 5.6. Окно **Смена пароля**

Копирование в другое хранилище — доступно только при администрировании ключей в файле. Для копирования ключа ЭЦП в другой файл хранилища необходимо выполнить следующие действия:

1. Выбрать файл хранилища, в который необходимо скопировать ключ ЭЦП. Для этого необходимо нажать кнопку **Выбрать** над вторым списком и в появившемся диалоговом окне указать нужный файл.
2. Выбрать нужный ключ ЭЦП в списке и нажать кнопку **Копировать**. При этом на экране откроется окно **Копирование ключа ЭЦП** (см. рис. 5.7), в котором необходимо ввести пароль на ключ. При вводе пароля учитывается раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). После поля ввода пароля отображается подсказка о текущей раскладке. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

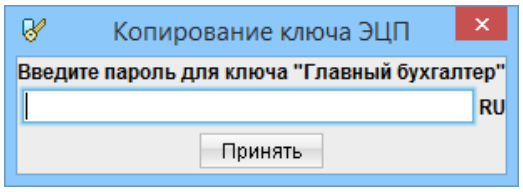


Рис. 5.7. Окно **Копирование ключа ЭЦП**

Внимание!

Если в файле хранилища, в который копируется ключ, уже имеется ключ с таким же наименованием, то будет выдан запрос на подтверждение сохранения ключа. В случае положительного ответа копируемый ключ будет записан в файл, а старый ключ с тем же названием будет безвозвратно утерян.

При администрировании ключей на USB-токене клиент также может проводить администрирование устройства:

Изменение наименования устройства. Для этого необходимо нажать кнопку **Переименовать** в блоке «Администрирование USB-токена». В результате на экране откроется окно **Смена наименования USB-токена** (см. рис. 5.8), в котором необходимо ввести новое наименование устройства.

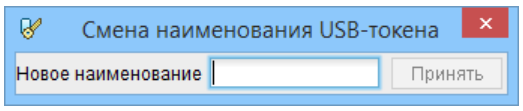


Рис. 5.8. Окно **Смена наименования USB-токена**

Изменение пароля к устройству. Для изменения пароля к устройству необходимо нажать кнопку **Изменить пароль**. В результате появится окно **Смена пароля USB-токена** (см. рис. 5.9), в котором необходимо ввести текущий и новый пароли. При вводе пароля учитываются раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

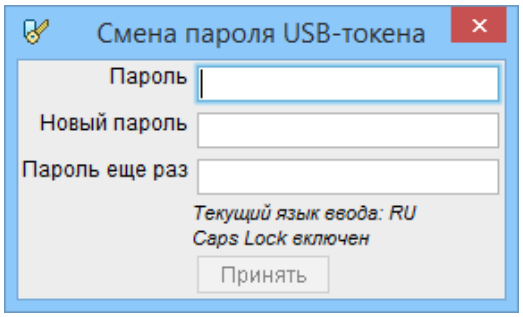


Рис. 5.9. Окно **Смена пароля USB-токена**

При вводе неверного текущего пароля несколько[1] раз подряд устройство будет заблокировано. При этом будут выполнены следующие действия:

- Если устройство не поддерживает возможность разблокирования, то будет выполнен переход на шаг выбора хранилища ключа.
- Если устройство поддерживает возможность разблокирования, то будет выполнен переход на шаг разблокирования устройства. Данный шаг аналогичен соответствующему шагу при регистрации нового клиента (подробнее см. в подразделе **Разблокирование USB-токена**).

Изменение кода разблокировки. Доступно только для устройств, которые поддерживают разблокирование. Для изменения кода разблокировки необходимо нажать кнопку **Изменить код разблокировки**. В результате появится окно **Смена кода разблокировки USB-токена** (см. рис. 5.10), в котором необходимо ввести текущий и новый коды разблокировки. При вводе кода учитываются раскладка клавиатуры (украинская, русская, латинская) и регистр (заглавные или строчные буквы). Под полями отображаются подсказки о текущей раскладке клавиатуры и включенной клавише **Caps Lock**.

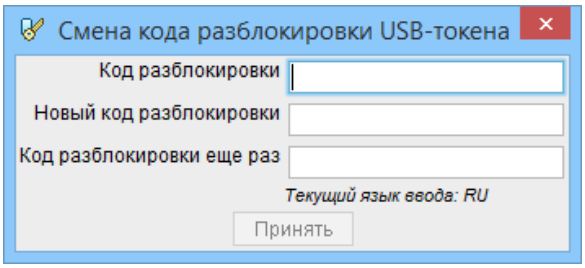


Рис. 5.10. Окно **Смена кода разблокировки USB-токена**

При вводе неверного кода разблокировки несколько[2] раз подряд устройство будет окончательно заблокировано. При этом будет выполнен возврат к шагу выбора хранилища ключа. Для получения дальнейших инструкций необходимо обратиться в отдел технической поддержки обслуживающего банка.

[1] Количество попыток ввода неверного пароля зависит от типа устройства.
[2] Количество попыток ввода неверного кода разблокировки зависит от типа устройства.

Раздел 6

Источники дополнительной информации

С дополнительной информацией по данной тематике можно ознакомиться в документах:

- ***PC-Банкинг для корпоративных клиентов. Регистрация в системе iBank 2 UA***
- ***Система iBank 2 UA. Internet-Банкинг для корпоративных клиентов. Руководство пользователя***
- ***Система iBank 2 UA. PC-Банкинг для корпоративных клиентов. Руководство пользователя***
- ***Система iBank 2 UA. Web-Банкинг для корпоративных клиентов. Руководство пользователя***
- ***Система iBank 2 UA. Internet-Банкинг для Центров финансового контроля. Руководство пользователя***
- ***Система iBank 2 UA. PC-Банкинг для Центров финансового контроля. Руководство пользователя***

Примечание:

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