Регистрация сотрудников банка в системе iBank 2 UA

ООО «БИФИТ Сервис»

(версия 2.0.21.3113)

Оглавление

Введение

Настоящий документ представляет собой руководство по использованию модуля АРМ **Регистратор банковских сотрудников** системы электронного банкинга iBank 2 UA. Данный модуль предназначен для предварительной регистрации банковских сотрудников и ключей ЭЦП в системе iBank 2 UA.

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

Необходимые действия сотрудника банка для входа в АРМ **Регистратор банковских сотрудников** описаны в разделе **Вход в систему**.

Подробное описание процедуры регистрации нового сотрудника банка представлено в разделе **Регистрация нового сотрудника банка**.

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

В разделе **Администрирование ключей ЭЦП** представлено описание возможностей АРМ **Регистратор банковских сотрудников** по управлению ключами ЭЦП сотрудников банка.

Раздел 1

Предварительная настройка

Требования к системе

Для работы с системой сотруднику банка 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 сотрудника банка USB-порта для использования съемных носителей информации. Съемный носитель информации (например, USB-токен[1]) необходим для хранения ключей ЭЦП сотрудника банка.

2. Установленный Web-браузер на компьютере сотрудника банка, 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 сотрудника банка виртуальной Java-машины, необходимо с Web-сайта компании-разработчика (http://www.java.com) скачать и установить дистрибутив программы.

   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 секретных ключей ЭЦП. В отличие от других съемных носителей, с USB-токена невозможно скопировать ключи ЭЦП, что существенно снижает возможность несанкционированного доступа к ключу ЭЦП сотрудника банка.

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

3. Наличие установленных драйверов для USB-токенов, если сотрудник банка использует USB-токены для хранения своих секретных ключей ЭЦП. Актуальные версии драйверов поддерживаемых USB-токенов можно скачать с сайта компании-разработчика (http://bifit.ua/downloads/index.html).

4. Доступ в Интернет. Рекомендуемая скорость соединения — 1 Мбит/сек.

Настройка подключения к Интернет

Для работы с системой iBank 2 UA сотруднику банка 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 сети. Поэтому для работы Java-апплетов в правилах фильтрации на Firewall необходимо открыть следующие TCP-порты:

- TCP-порт для соединения Web-браузера сотрудника банка с Web-сервером банка по протоколу SSL (для этого соединения обычно используется порт 443);

- TCP-порт для работы Java-апплета **Регистратор банковских сотрудников** 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 администратором сети 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 сотруднику банка необходимо зарегистрироваться в системе. Процесс регистрации сотрудника в iBank 2 UA включает в себя предварительную (через Интернет) и окончательную регистрацию.

Предварительная регистрация выполняется в АРМ **Регистратор банковских сотрудников**, 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 администратором системы и может отличаться от стандартного.

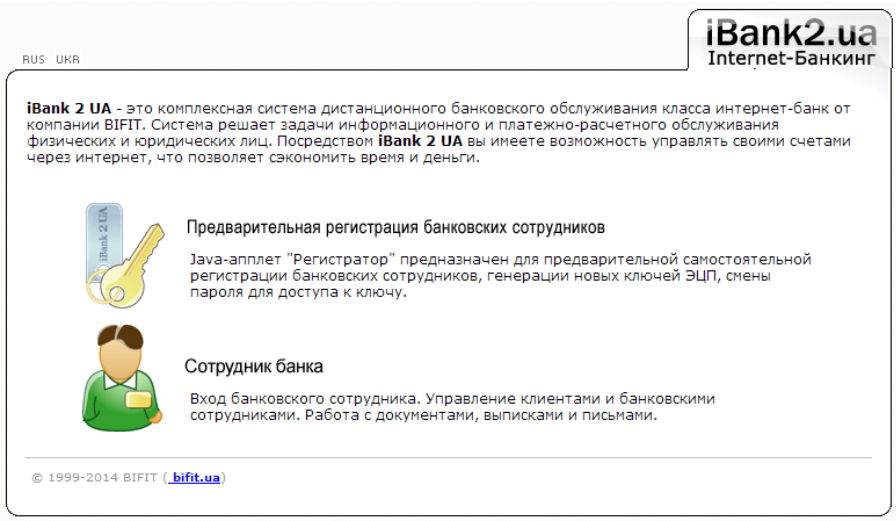


Рис. 2.1. Главная страница системы iBank 2 UA

На главной странице iBank 2 UA необходимо выбрать пункт **Предварительная регистрация банковских сотрудников**, 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 банковских сотрудников** представляет собой последовательность шагов, которые необходимо выполнить для предварительной регистрации сотрудника банка, новой пары ключей ЭЦП и т. п. Внешний вид и состав шагов настраиваются администратором системы и могут отличаться от описанных шагов в данном документе.

В результате на экране появится окно АРМ **Регистратор банковских сотрудников** на шаге подключения к банковскому серверу с использованием proxy-сервера (см. рис. 2.3). Если для доступа к сети Интернет используется proxy-сервер, то сотруднику банка 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**.

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

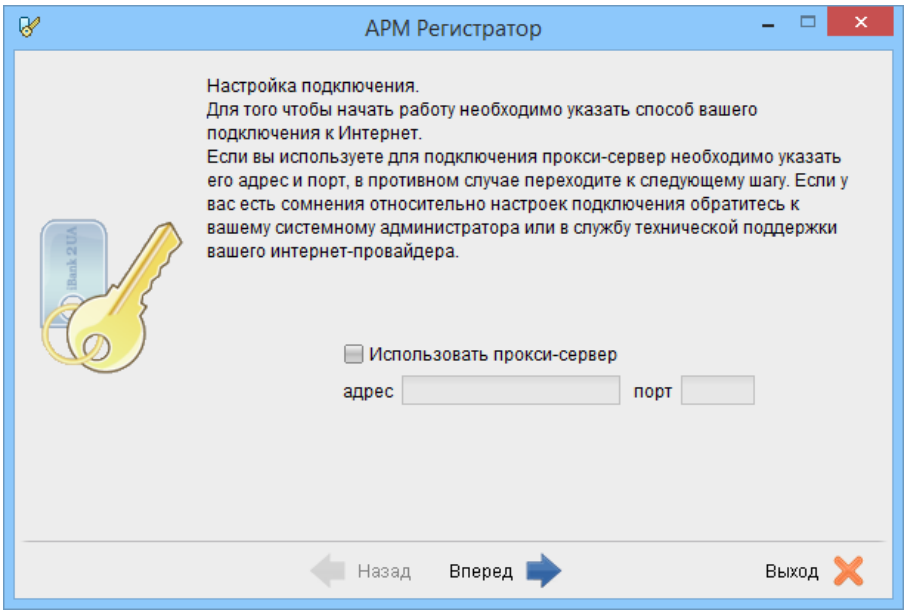


Рис. 2.3. Шаг настройки подключения к банковскому серверу

Выбор раздела АРМ

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

1. ***Новый сотрудник банка*** — переход к предварительной регистрации сотрудника банка;
2. ***Новые ключи ЭЦП*** — переход к генерации новой пары ключей ЭЦП;

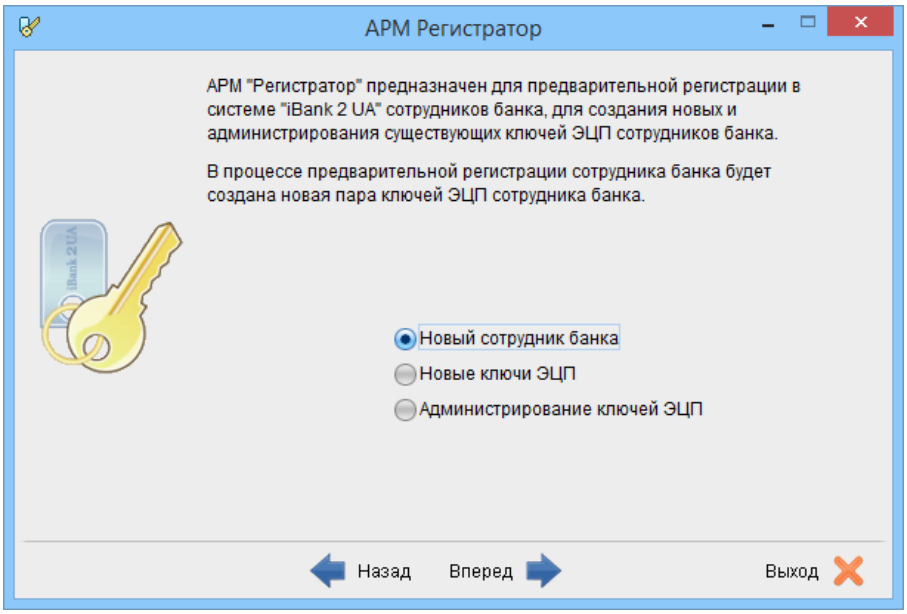


Рис. 2.4. Шаг выбора раздела АРМ **Регистратор банковских сотрудников**

3. ***Администрирование ключей ЭЦП*** — переход к разделу управления ключами ЭЦП сотрудника банка.

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

Раздел 3

Регистрация нового сотрудника банка

Предварительная регистрация в АРМ Регистратор банковских сотрудников

Предварительная регистрация сотрудника банка заключается в последовательном заполнении ряда экранных форм в АРМ **Регистратор банковских сотрудников**.

Заполнение информации о сотруднике банка

После выбора пункта **Новый сотрудник банка** на шаге выбора раздела АРМ, выполняется переход на шаг заполнения реквизитов сотрудника банка (см. рис. 3.1). Табельный номер не обязателен для заполнения.

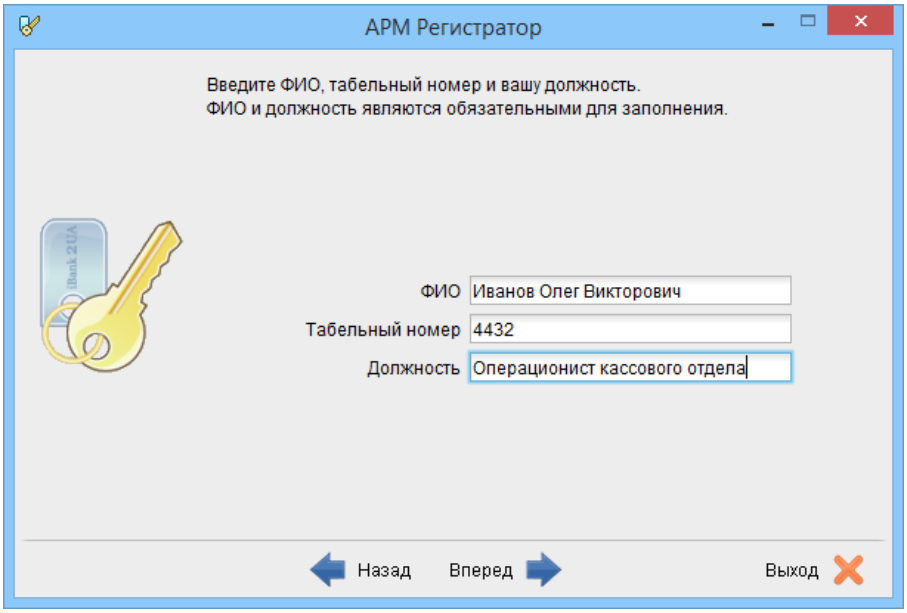


Рис. 3.1. Шаг ввода реквизитов сотрудника банка

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

Проверка введенной информации

После заполнения информации о сотруднике банка выполняется переход на шаг проверки введенной информации (см. рис. 3.2). Если при проверке будет обнаружена ошибка, то необходимо нажатием кнопки **Назад** вернуться на предыдущий шаг для ее исправления.

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

Выбор хранилища ключа ЭЦП

При регистрации нового сотрудника банка для него автоматически генерируется новая пара ключей ЭЦП.

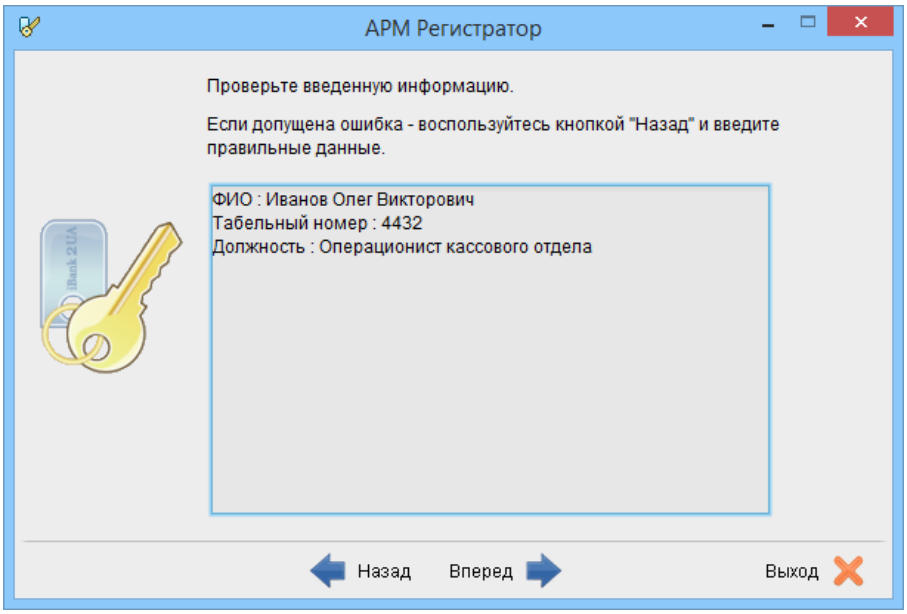


Рис. 3.2. Шаг проверки введенной информации о сотруднике банка

После проверки введенной информации о сотруднике банка выполняется переход на шаг выбора хранилища ключа ЭЦП (см. рис. 3.3). 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.

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

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

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. 3.4). 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 сотруднику банка в дальнейшей работе (например, при выборе хранилища ключа в окне **Вход в систему** АРМ **Сотрудник банка** (описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство сотрудника банка***)).
- Пароль на устройство. Минимальная длина составляет 6 символов.

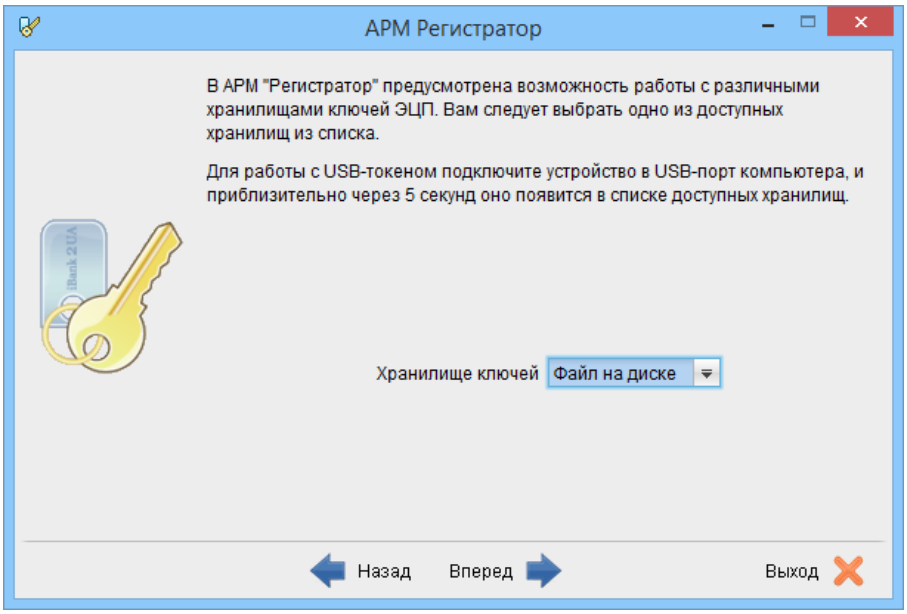


Рис. 3.3. Шаг выбора хранилища ключа ЭЦП

- Код разблокировки. Отображается, если устройство поддерживает возможность разблокирования. Минимальная длина составляет 8 символов.

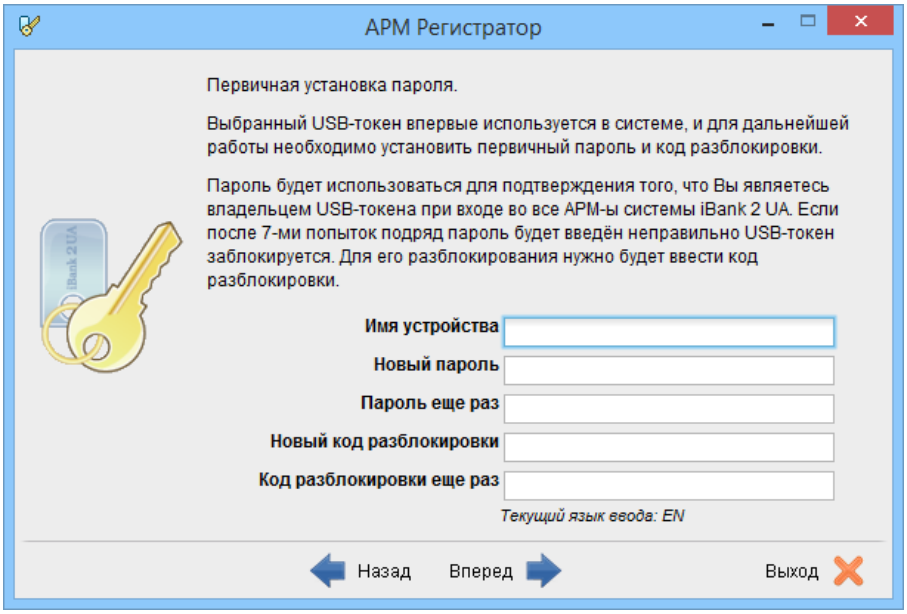


Рис. 3.4. Шаг первичной инициализации USB-токена

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. 3.5).

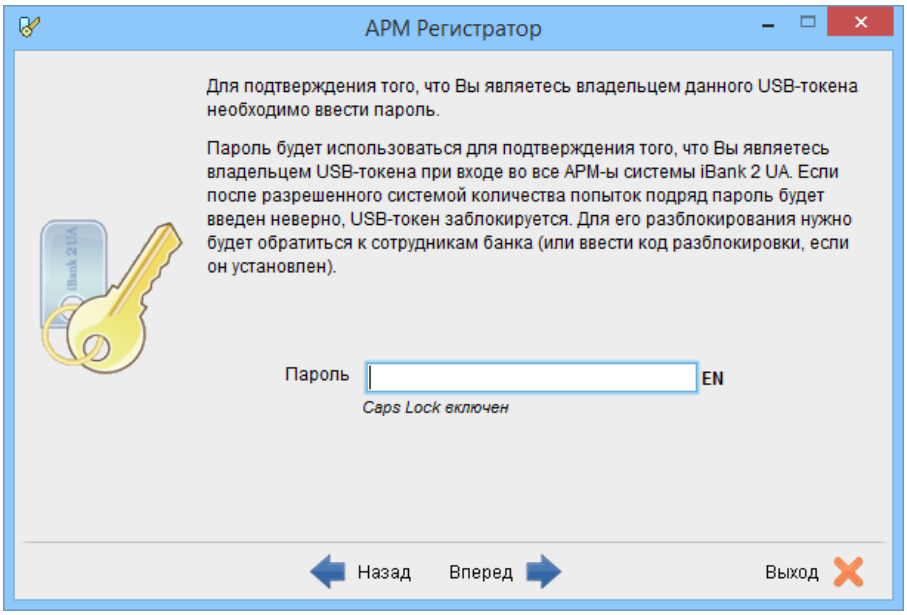


Рис. 3.5. Шаг ввода пароля на USB-токен

При вводе пароля учитываются текущая 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[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 к администратору системы за дальнейшими инструкциями.

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

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. 3.6).

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 разблокировки несколько[2] раз подряд устройство будет окончательно заблокировано. Для получения дальнейших инструкций необходимо обратиться к администратору системы.

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

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

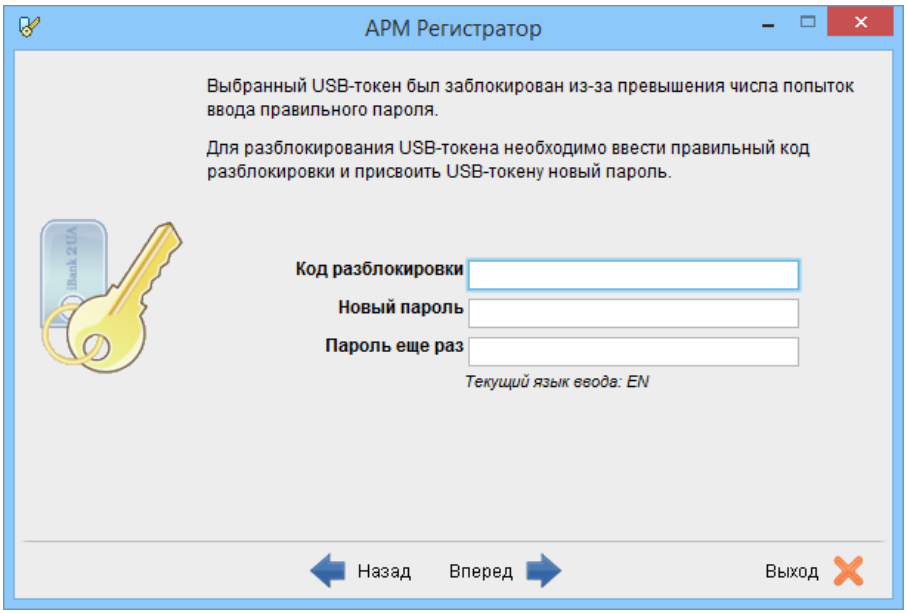


Рис. 3.6. Шаг разблокирования USB-токена

Ввод наименования ключа

После первичной инициализации, ввода пароля к устройству или его разблокирования, выполняется переход на шаг ввода наименования ключа ЭЦП (см. рис. 3.7).

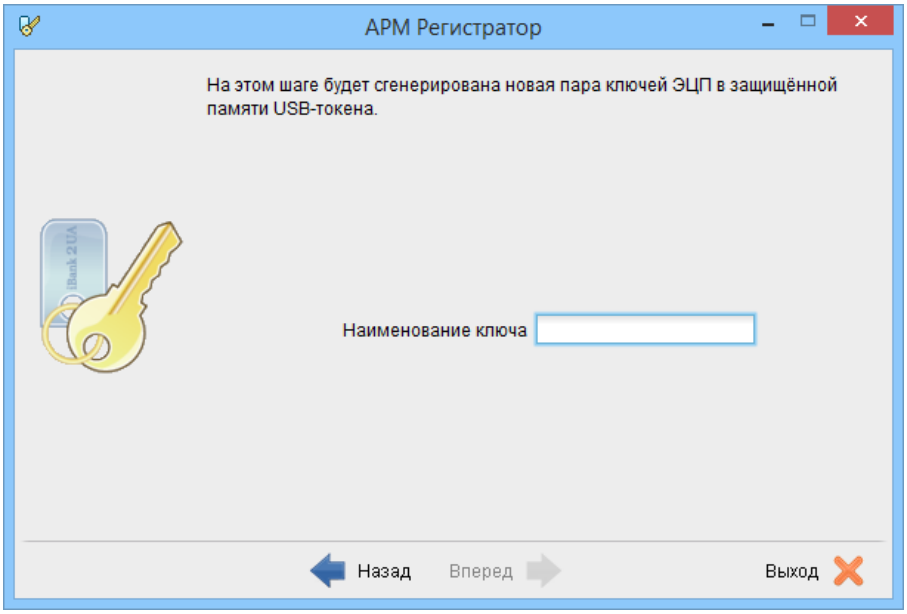


Рис. 3.7. Шаг ввода наименования ключа ЭЦП

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. 3.8). В ходе тестирования проверяется правильность записи секретного ключа ЭЦП сотрудника банка на устройство и корректность регистрации открытого ключа ЭЦП в банке.

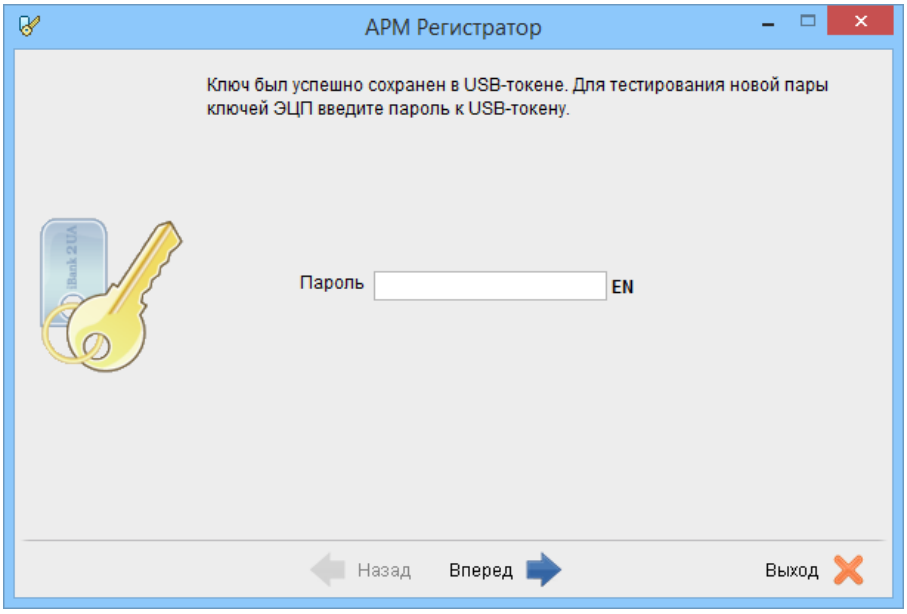


Рис. 3.8. Шаг тестирования ключа на USB-токене

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 ЭЦП. Если возможность разблокирования устройства не поддерживается, то необходимо обратиться к администратору системы.

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. 3.9). В одном файле могут храниться несколько ключей ЭЦП одного или разных клиентов.

Для выбора файла хранилища ключа ЭЦП можно воспользоваться двумя способами:

- Ввести вручную путь к файлу хранилища ключа ЭЦП.

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

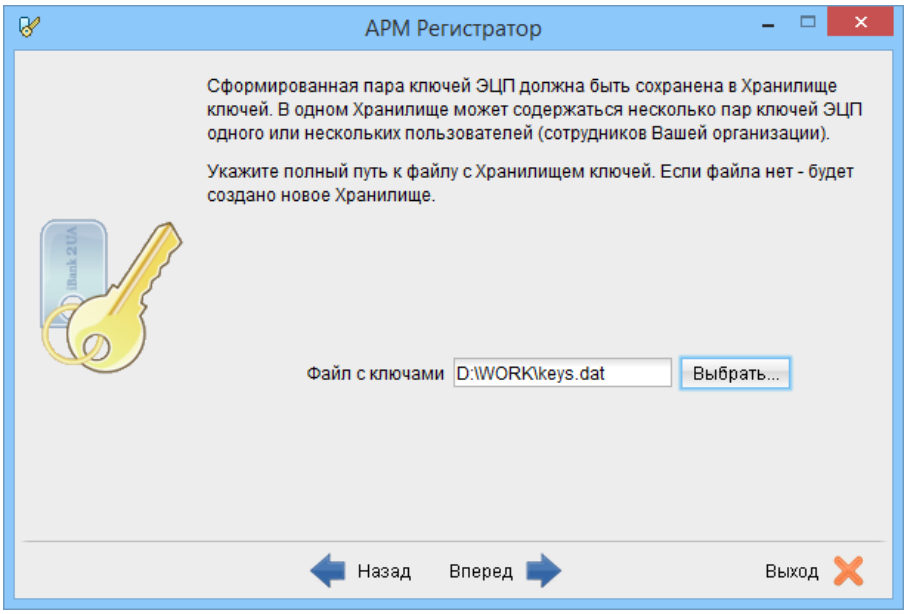


Рис. 3.9. Шаг выбора файла хранилища ключа ЭЦП

- Нажать кнопку **Выбрать...**, в результате чего на экране откроется стандартное диалоговое окно 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. 3.10).

Наименование ключа можно указать двумя способами:

- Ввести вручную;
- 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. 3.11).

> ***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 сотруднику банка в дальнейшей работе (например, при выборе ключа ЭЦП в окне **Вход в систему** АРМ **Сотрудник банка** (описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство сотрудника банка***)).

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**.

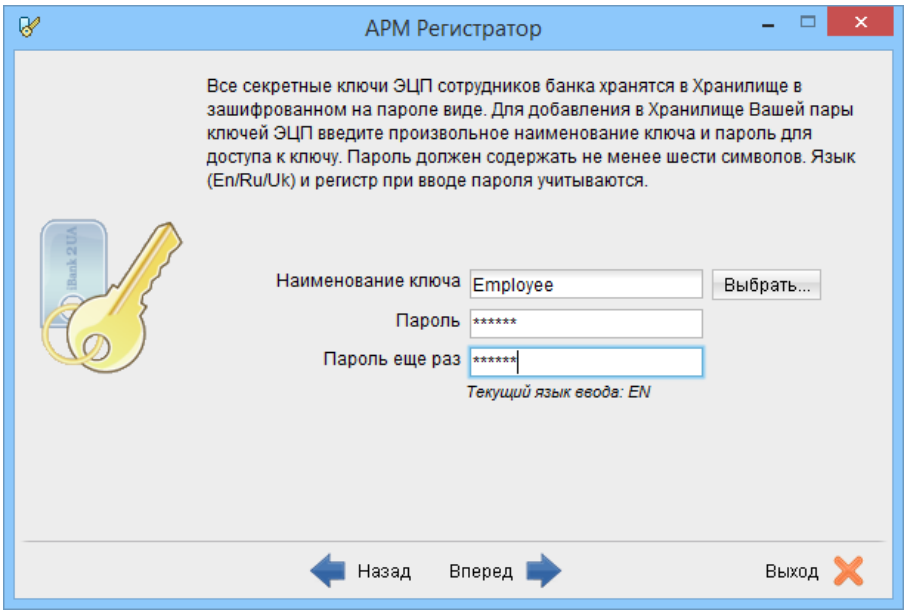


Рис. 3.10. Шаг ввода наименования и пароля ключа ЭЦП в файле

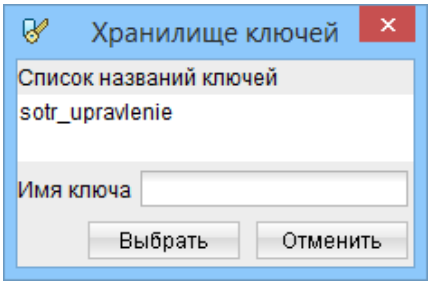


Рис. 3.11. Список ключей ЭЦП, которые содержатся в файле

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. 3.12). В ходе тестирования проверяется правильность записи секретного ключа ЭЦП сотрудника банка в файл хранилища ключа и корректность регистрации открытого ключа ЭЦП в банке.

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 идентификатор сгенерированного открытого ключа ЭЦП, а также отметка **Распечатать сертификат** (см. рис. 3.13).

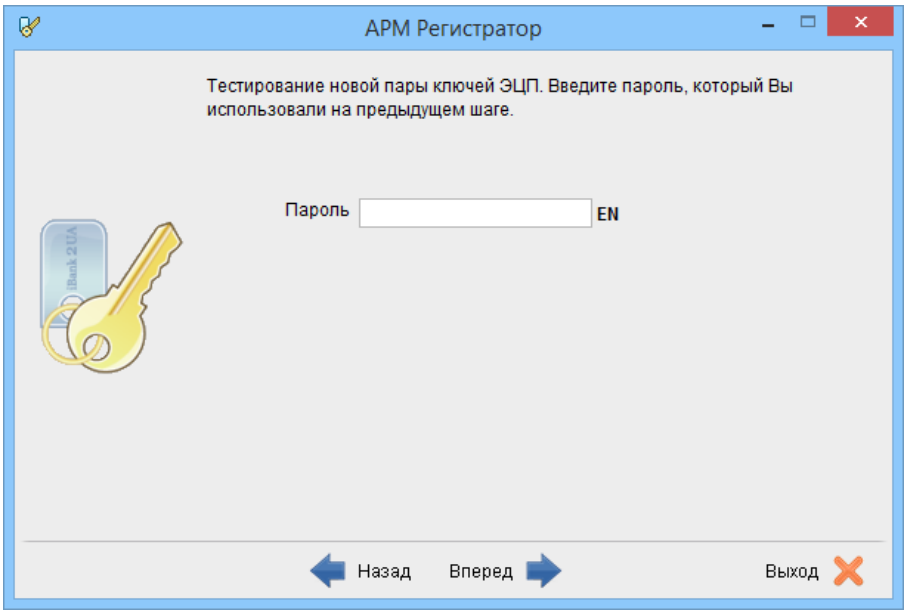


Рис. 3.12. Шаг тестирования новой пары ключей ЭЦП

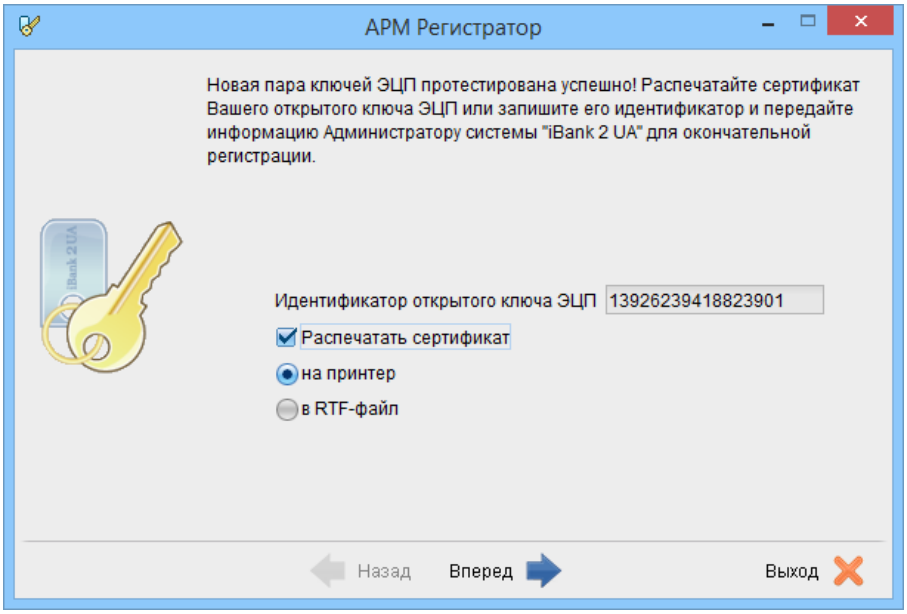


Рис. 3.13. Шаг печати сертификата открытого ключа ЭЦП

При нажатии кнопки **Далее** выполняется переход на финальный шаг регистрации (см. рис. 3.14) с дальнейшими инструкциями для окончательной регистрации сотрудника банка в системе iBank 2 UA. Если была включена отметка **Распечатать сертификат**, то также выполняется печать сертификата открытого ключа ЭЦП. Печать сертификата возможна на принтер или в RTF-файл.

На этом процесс предварительной регистрации сотрудника банка в АРМ **Регистратор банковских сотрудников** завершен, при этом он приобретает в системе iBank 2 UA статус Новый.

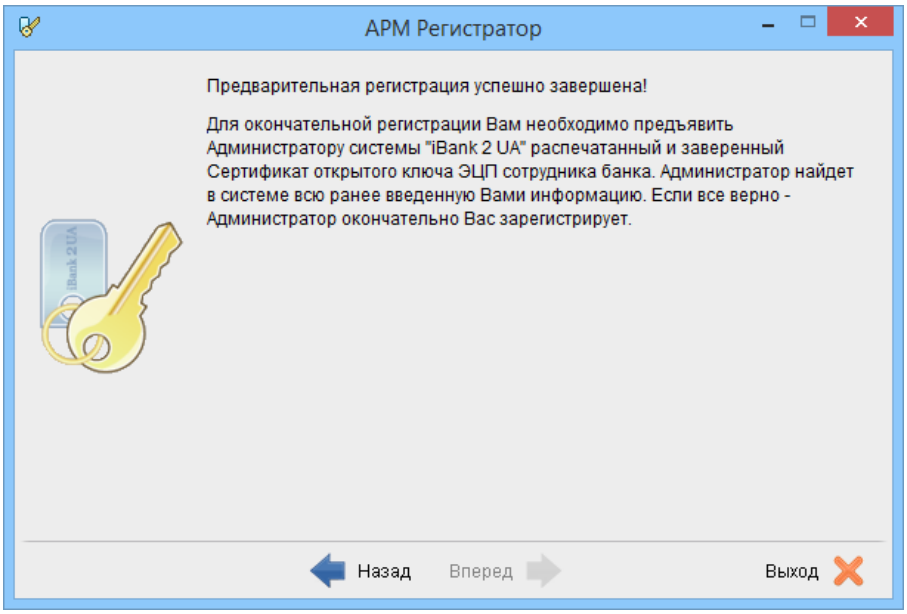


Рис. 3.14. Финальный шаг регистрации

Внимание!

Информация о вновь зарегистрированном сотруднике банка хранится в системе в течении срока, определенного администратором системы (по умолчанию 30 дней). Если к моменту окончания этого срока сотрудник банка не прошел окончательную регистрацию, то информация о нем удаляется с банковского сервера.

Окончательная регистрация

Окончательная регистрация сотрудника банка в системе iBank 2 UA может быть выполнена уполномоченным сотрудником банка в АРМ **Сотрудник банка** (подробное описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство сотрудника банка***) или администратором системы в АРМ **Администратор системы** (подробное описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство администратора системы***). Для этого сотруднику банка необходимо предъявить распечатанный и заверенный сертификат открытого ключа ЭЦП или записанный идентификатор открытого ключа ЭЦП.

В процессе окончательной регистрации уполномоченный сотрудник банка или администратор системы выполнит следующие действия:

- Проверит и в случае необходимости откорректирует информацию, введенную сотрудником банка в процессе предварительной регистрации.
- Установит сотруднику банка роль в системе iBank 2 UA.
- Установит сотруднику банка права на работу с определенными банковскими подразделениями, видами документов, отчетов и клиентами.
- Активирует открытый ключ ЭЦП сотрудника банка.

Раздел 4

Регистрация ключей ЭЦП

Создание новых ключей ЭЦП

Процедура создания новой пары ключей ЭЦП заключается в последовательном заполнении ряда экранных форм в АРМ **Регистратор банковских сотрудников**. 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 выполняется переход на шаг выбора типа хранилища ключа ЭЦП. Данный шаг и все последующие шаги аналогичны соответствующим шагам при регистрации нового сотрудника банка (подробнее см. в подразделе **Выбор хранилища ключа ЭЦП**).

Внимание!

Предварительно зарегистрированный открытый ключ ЭЦП сотрудника банка хранится в системе в течении срока, определенного администратором системы (по умолчанию 30 дней). Если к моменту окончания этого срока ключ ЭЦП не прошел окончательную регистрацию, то информация о ключе удаляется с банковского сервера.

Окончательная регистрация новой пары ключей ЭЦП

Окончательная регистрация новой пары ключей ЭЦП сотрудника банка выполняется уполномоченным сотрудником банка в АРМ **Сотрудник банка** (подробное описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство сотрудника банка***) или администратором системы в АРМ **Администратор системы** (подробное описание работы в данном АРМ представлено в документации ***Система iBank 2 UA. Руководство сотрудника банка***). Для этого сотрудник банка предъявляет распечатанный и заверенный сертификат открытого ключа ЭЦП или записанный идентификатор открытого ключа ЭЦП. Уполномоченный сотрудник банка или администратор системы находит в системе информацию об открытом ключе ЭЦП сотрудника банка, сверяет ее с информацией в сертификате (или проверяет совпадение идентификатора, предъявленного сотрудником банка). Если не будет обнаружено ошибок, то он зарегистрирует в системе и активирует новую пару ключей ЭЦП.

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 сотрудника банка (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 сотрудника банка (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 сотрудника банка (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).

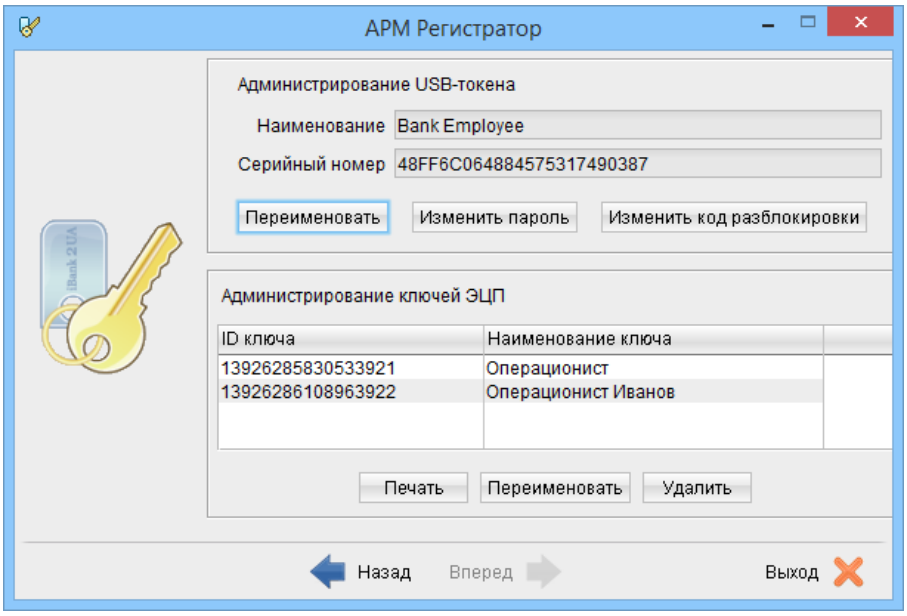


Рис. 5.1. Шаг администрирования ключей ЭЦП на USB-токене

- 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 диалоговом окне указать нужный файл.

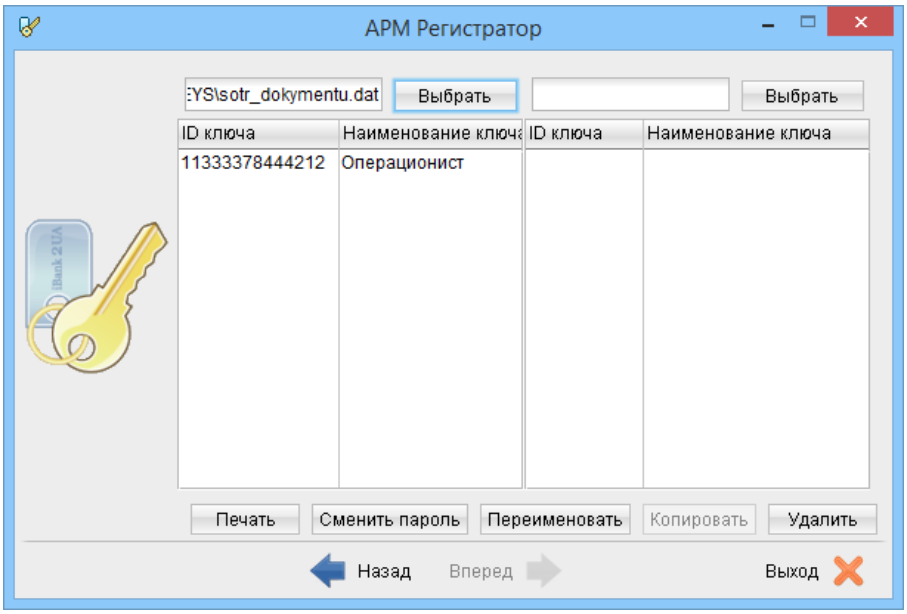


Рис. 5.2. Шаг администрирования ключей ЭЦП в файле

В АРМ **Регистратор банковских сотрудников** 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.

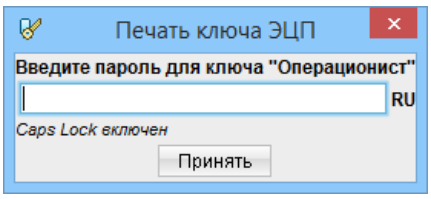
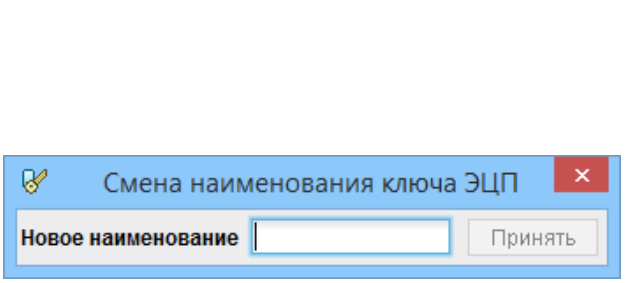


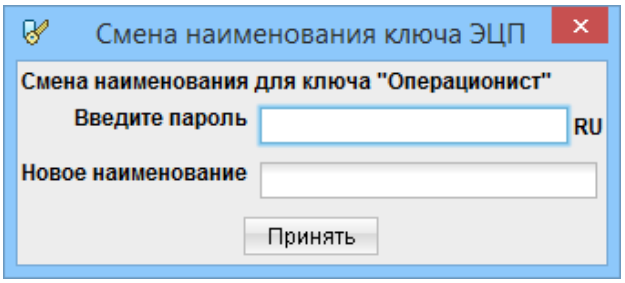
Рис. 5.3. Окно **Печать ключа ЭЦП**

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**.



а) Ключ на USB-токене



б) Ключ в файле на диске

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

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 (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.

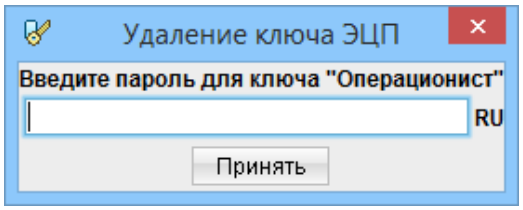


Рис. 5.5. Окно **Удаление ключа ЭЦП**

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 **Переименовать**. 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**.

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

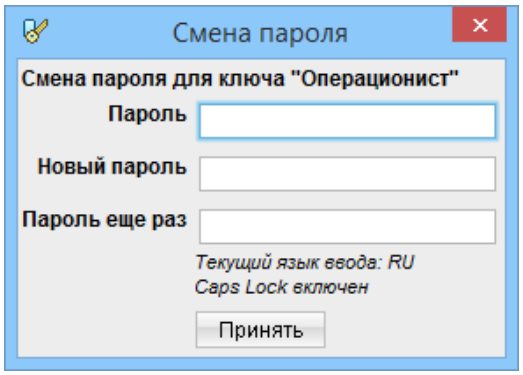


Рис. 5.6. Окно **Смена пароля**

поля ввода пароля отображается подсказка о текущей раскладке. При включенной клавише **Caps Lock** соответствующая подсказка отображается под полем.

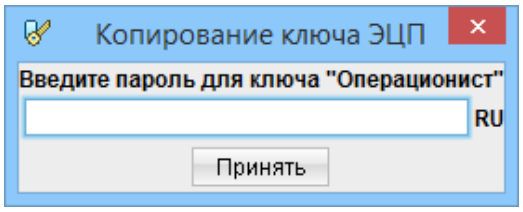


Рис. 5.7. Окно **Копирование ключа ЭЦП**

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 сотрудник банка 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.

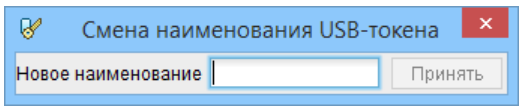


Рис. 5.8. Окно **Смена наименования USB-токена**

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 с текущей раскладкой клавиатуры и включенной клавише **Caps Lock**.

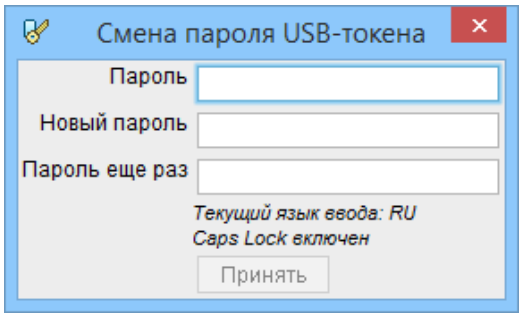


Рис. 5.9. Окно **Смена пароля USB-токена**

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 сотрудника банка (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**.

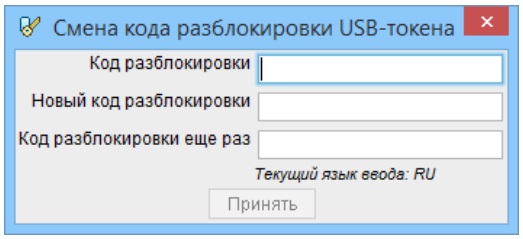


Рис. 5.10. Окно **Смена кода разблокировки USB-токена**

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 к администратору системы.

[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:

- ***Система iBank 2 UA. Руководство сотрудника банка***
- ***Система iBank 2 UA. Руководство администратора системы***

Примечание:

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