КОМПАНИЯ CS

iFOBS

Интерактивная система фронт-офисного обслуживания клиентов банка

Инструкция по работе с сертификатами и ключами

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Настоящий документ представляет собой инструкцию для пользователей системы iFOBS (Windows-версия) по работе с сертификатами, ключами и паролями. В документе описан порядок действий пользователя по получению и смене сертификатов при первом входе в систему, последующей работе с сертификатами в системе.

2. ОБЩИЕ ПОЛОЖЕНИЯ

2.1. Создание учетной записи пользователя администратором iFOBS

Во время создания новой учетной записи пользователя iFOBS администратор системы:

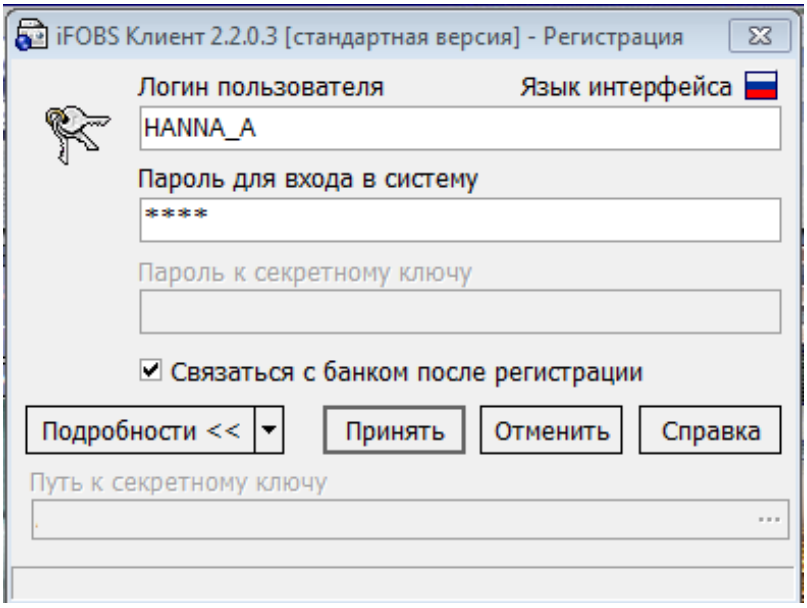
1. Указывает логин пользователя.
2. Задает пароль для первого входа пользователя в систему.
3. Выдает права пользователю на работу с системой и счетами.

3. РАБОТА С СЕРТИФИКАТАМИ В WINDOWS-ВЕРСИИ IFOBS

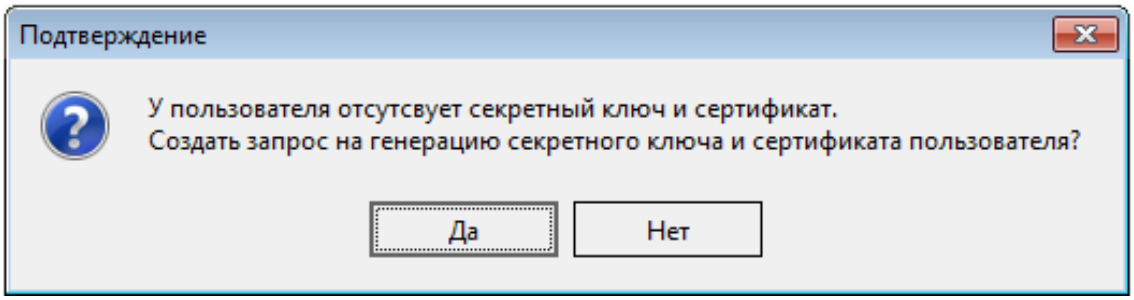
3.1. Первый вход и генерация сертификатов

Для первого входа в систему:

1. Запустите Windows-приложение iFOBS.
2. В поля **Логин пользователя** и **Пароль для входа в систему** введите логин и пароль для входа, выданные вам администратором системы (см. «Создание учетной записи пользователя администратором iFOBS»).

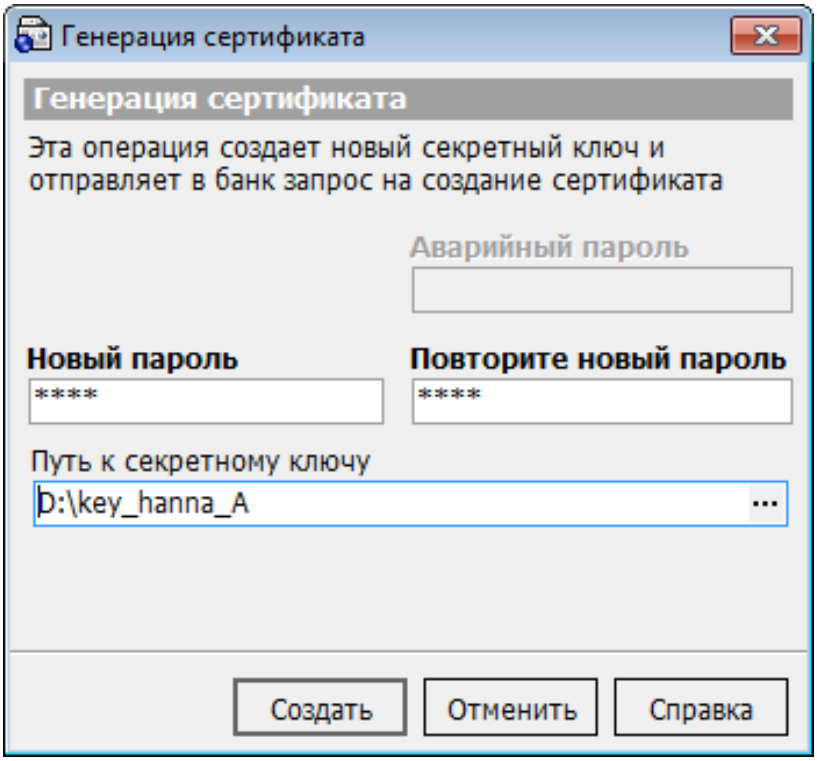


3. После ввода логина и пароля при первом входе система выдаст вам уведомление об отсутствии секретного ключа и сертификата и предложит вам их сгенерировать. Для продолжения работы нажмите кнопку «**Да**».

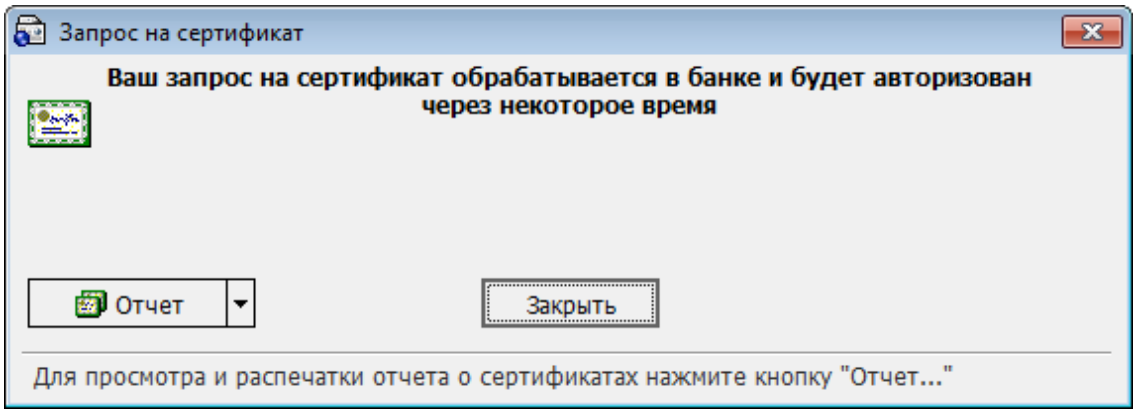


4. В открывшейся форме «Генерация сертификата» придумайте и введите пароль для секретного ключа в поля **Новый пароль** и **Повторите новый пароль**. В поле **Путь к секретному ключу** укажите путь, по которому будет сохранен ваш секретный ключ. Нажмите кнопку «**Создать**».

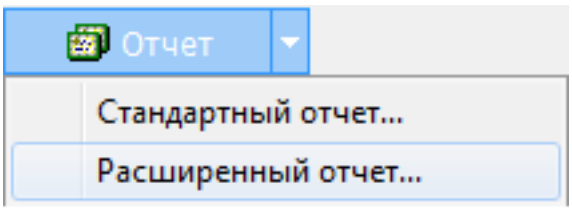
   Обратите внимание: пароли должны быть уникальны для каждого пользователя данного рабочего места в течение всего времени работы системы, должны содержать от 6 до 20 символов, должны содержать только латинские буквы разных регистров, цифры и символы: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Все прочие символы, пробел и кириллица игнорируются.



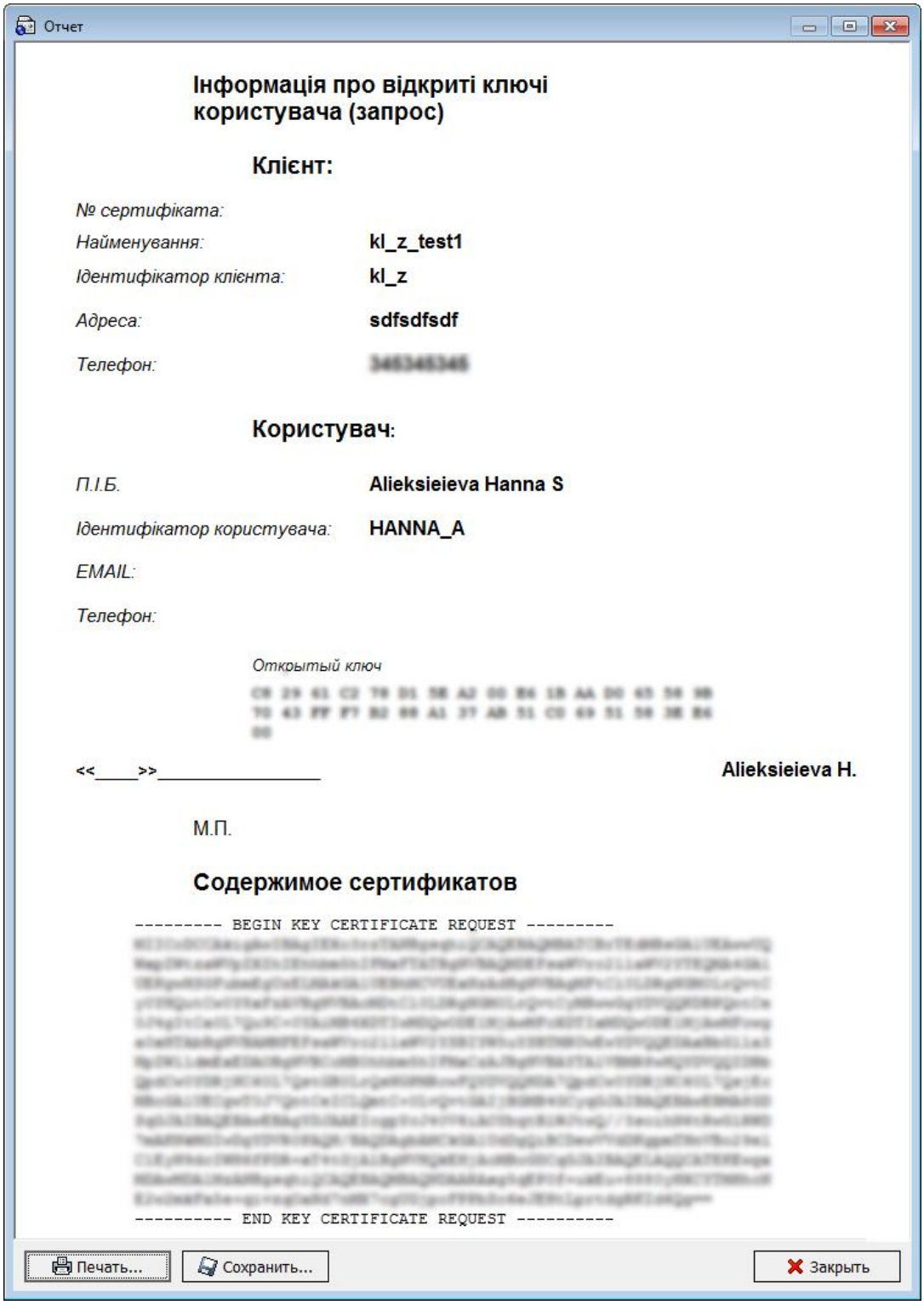
5. Система отобразит сообщение об отправке запроса на авторизацию сертификата в банк. После авторизации вы сможете использовать сертификат для входа в систему (см. «Авторизация и вход»).



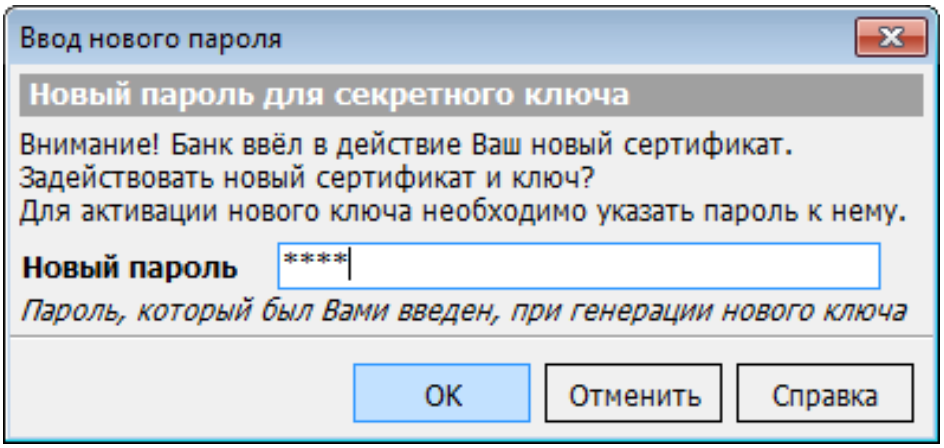
6. Для просмотра и распечатки отчета о сертификатах, нажмите кнопку «**Отчет**» и из выпадающего списка выберите нужный вид отчета: стандартный или расширенный:



7. В новой форме отобразится информация о сертификатах. После этого вам будет необходимо распечатать (кнопка «**Печать**») и подписать сертификат, заверить его печатью (при необходимости) и предоставить бланк в банк. Также вы можете сохранить информацию о сертификатах на локальном устройстве (кнопка «**Сохранить**»):



8. После авторизации сертификата запустите Windows-приложение iFOBS, введите свой логин и пароль. Система отобразит уведомление об активации нового сертификата и предложит указать пароль к нему. Введите пароль, который вы указывали при генерации сертификата в поле **Новый пароль**:



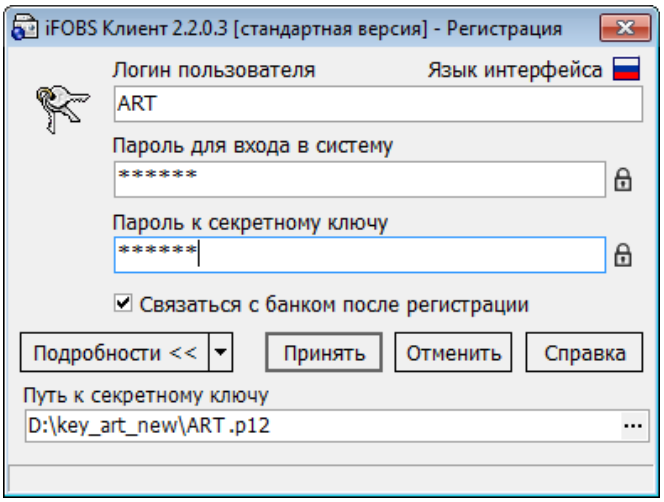
9. После нажатия кнопки **«ОК»** новый сертификат будет активирован.

3.2. Текущая работа с сертификатами

3.2.1. Авторизация и вход

Для входа в систему:

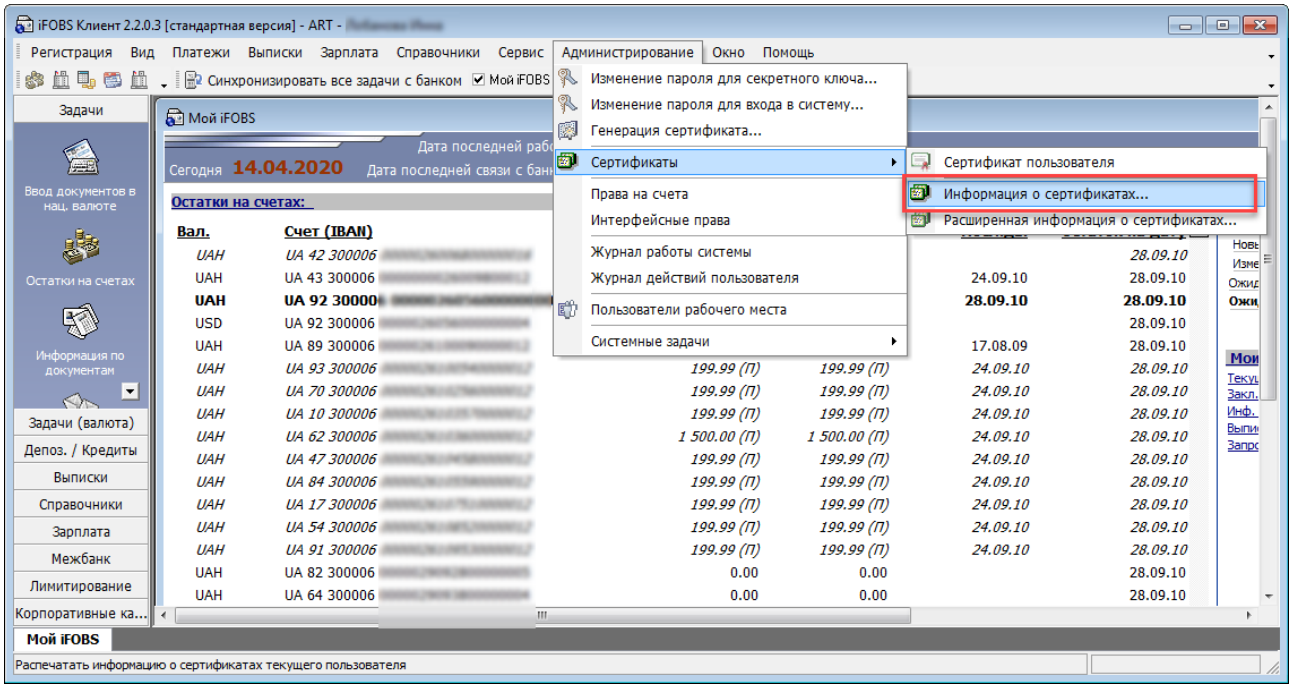
1. Запустите Windows-приложение iFOBS.
2. Введите свой логин, пароль для входа в систему.
3. Введите пароль и укажите путь к секретному ключу – кнопка ...
4. Нажмите кнопку «**Принять**».



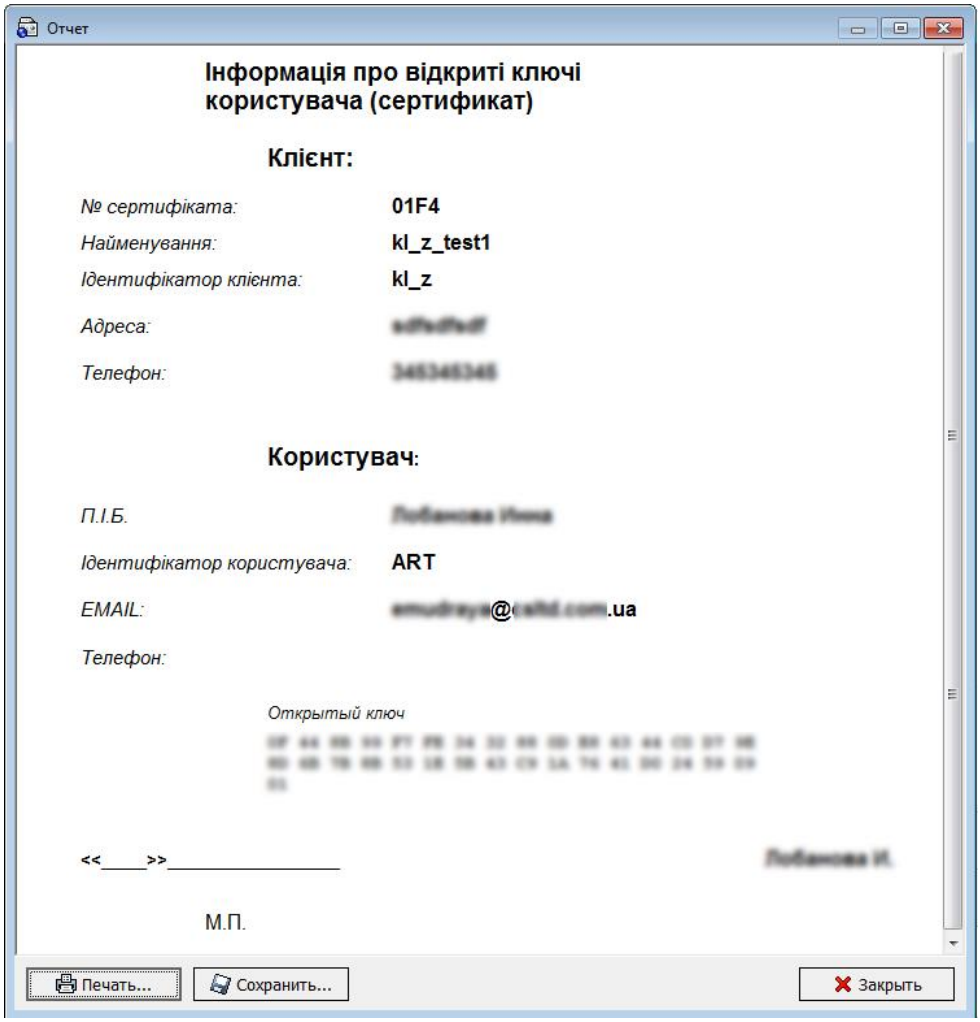
Если все данные были введены верно, будет осуществлен вход в систему. Если были указаны ошибочные данные, система отобразит сообщение об ошибке.

3.2.2. Просмотр информации о сертификатах

Для просмотра информации о сертификатах выберите меню **Администрирование/*Сертификаты/Информация о сертификатах***.



Информация о действующем сертификате открывается в режиме предварительного просмотра. При необходимости вы можете распечатать файл (кнопка «**Печать**») или сохранить его в формате .rtf (кнопка «**Сохранить**»).



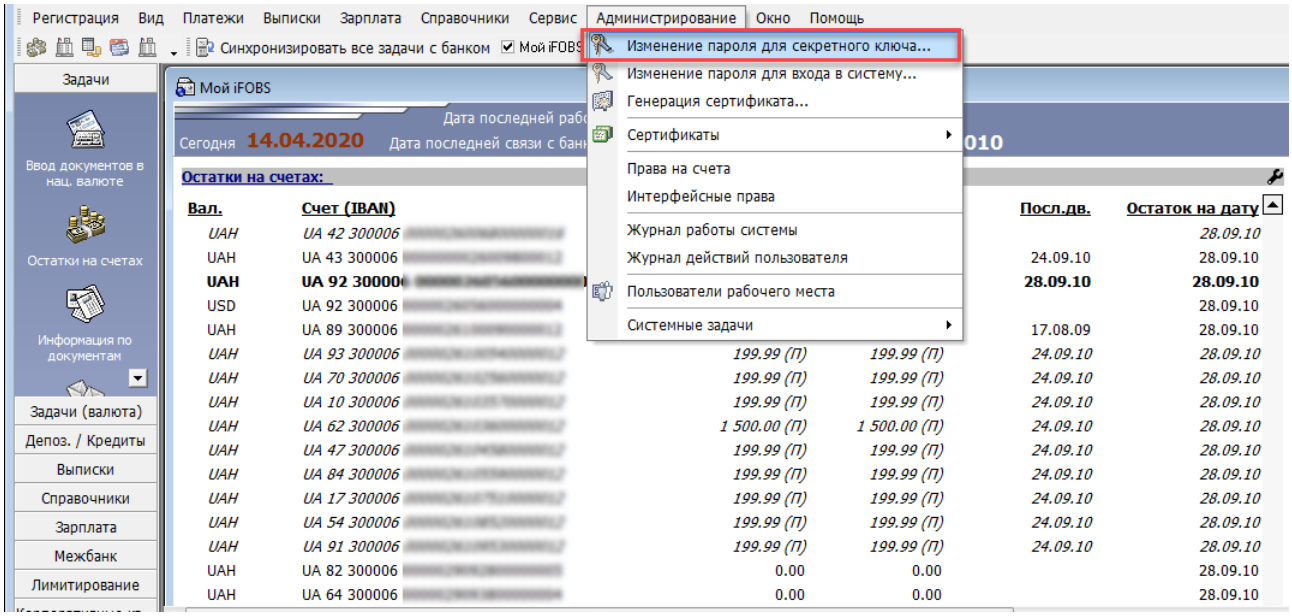
Для выхода из режима предварительного просмотра нажмите кнопку **«Закрыть»**.

3.2.3. Смена пароля на секретный ключ

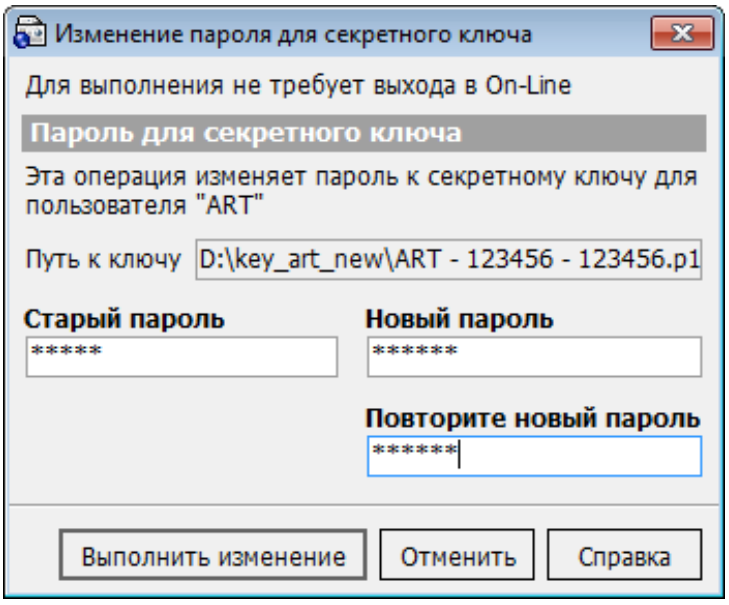
В процессе работы с системой у вас может возникнуть необходимость смены пароля к секретному ключу.

Для смены пароля на секретный ключ:

1. Выберите меню ***Администрирование/Изменение пароля для секретного ключа***:



2. В открывшейся форме введите свой пароль к секретному ключу в поле **Старый пароль**.
3. Придумайте и введите новый пароль в поля **Новый пароль** и **Повторите новый пароль**:

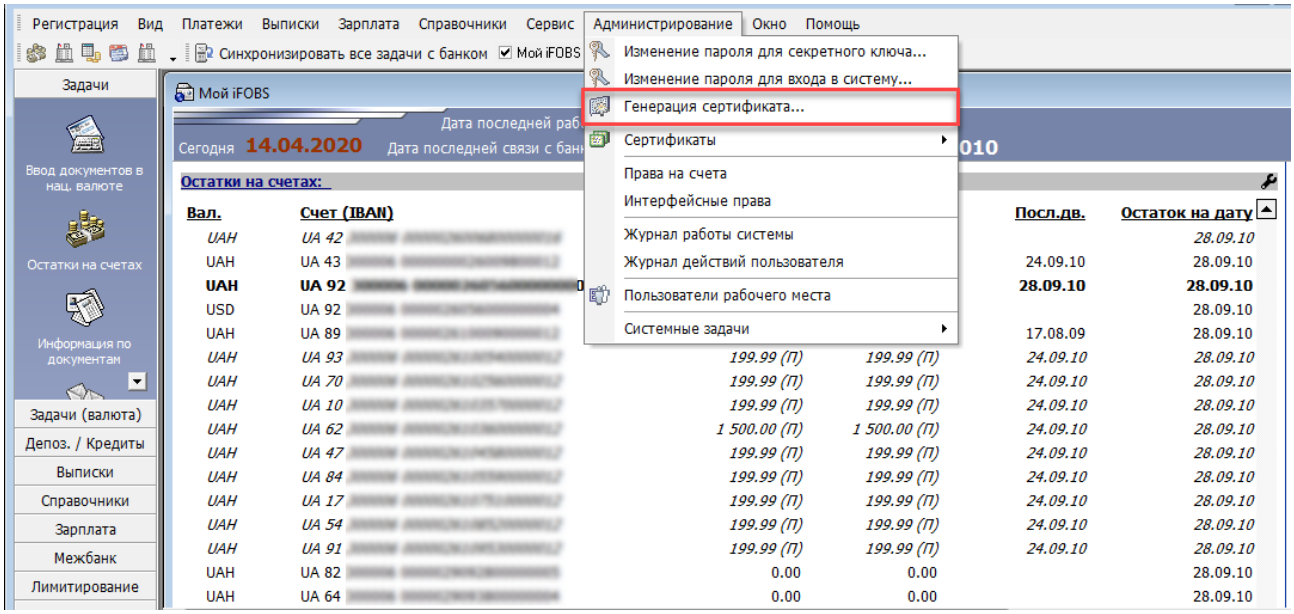


Обратите внимание: система требует, чтобы пароли были уникальны для каждого пользователя данного рабочего места в течение всего времени работы системы, содержали от 6 до 20 символов, содержали только латинские буквы разных регистров, цифры и символы: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Все прочие символы, пробел и русские буквы игнорируются.

4. Для изменения пароля нажмите кнопку **«Выполнить изменение»**;
5. Если смена пароля прошла успешно, система выдаст соответствующее сообщение.

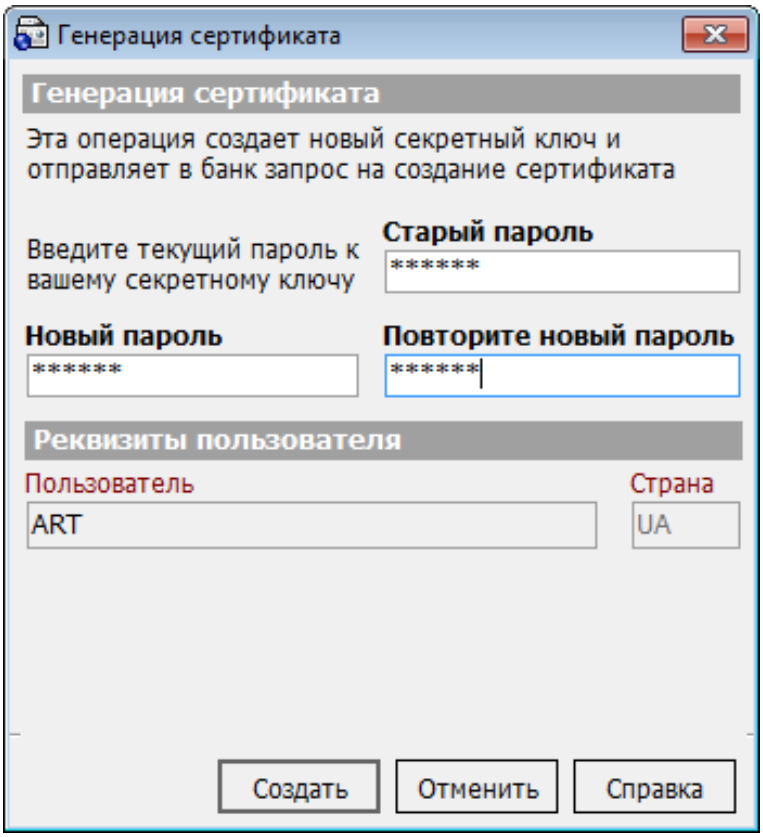
3.2.4. Плановая смена сертификата

Чтобы отправить в банк запрос на новый сертификат, выберите меню **Администрирование/*Генерация сертификата.***



<u>Для создания запроса на новый сертификат:</u>

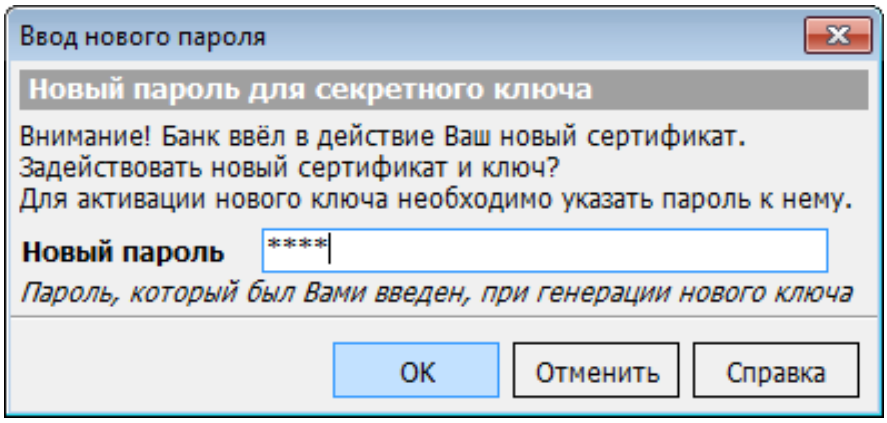
1. В открывшейся форме введите свой пароль к секретному ключу в поле **Старый пароль**.
2. Придумайте и введите новый пароль в поля **Новый пароль** и **Повторите новый пароль**.



Обратите внимание: система требует, чтобы пароли были уникальны для каждого пользователя данного рабочего места в течение всего времени работы системы, содержали от 6 до 20 символов, содержали только латинские буквы разных регистров,

цифры и символы: ! " # $ % & ' ( ) * + , - . / : ; < = > ? @ [\ ] ^ _ ` { | } ~ Все прочие символы, пробел и русские буквы игнорируются.

3. Для генерации запроса на сертификат нажмите кнопку **«Создать»**.
4. Если сертификат создан успешно, система выдаст соответствующее сообщение.
5. После нажатия в окне сообщения кнопки **«Да»** откроется форма активации нового ключа. Для активации введите **новый** пароль на секретный ключ в поле **Новый пароль** и нажмите кнопку **«ОК»**.

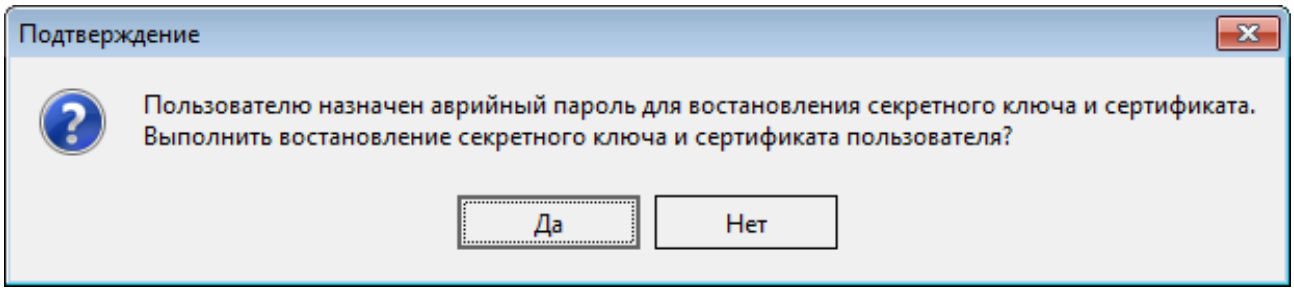


3.2.5. Аварийное получение новых сертификатов и ключей (восстановление доступа к системе)

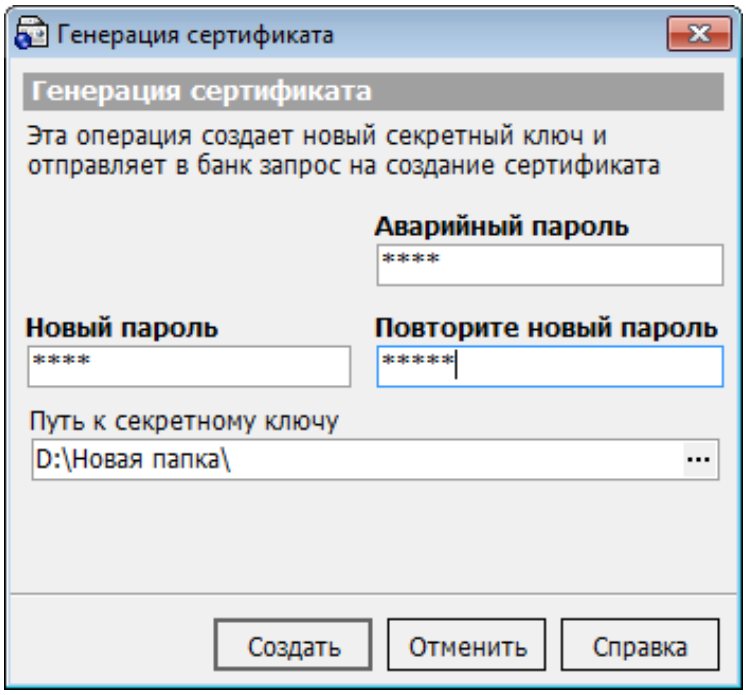
Если срок действия ваших сертификатов истек, вы забыли пароль к секретному ключу или ключи повреждены, вам необходимо обратиться в банк и получить у администратора системы **аварийный пароль**.

Для создания запроса на новый сертификат:

1. После получения от администратора системы аварийного пароля, войдите в систему iFOBS. Для этого на форме входа в систему введите свой логин и пароль на вход (см. «Авторизация и вход»).
2. Система отобразит сообщением, что для данного пользователя назначен аварийный пароль. Нажмите кнопку **«Да»**.



3. После этого произойдет автоматический переход на форму генерации нового сертификата.
4. Введите аварийный пароль в соответствующее поле, затем придумайте новый пароль к секретному ключу, введите его в поле **Новый пароль** и продублируйте в поле **Повторите новый пароль**.
5. Нажмите кнопку **«Создать»**.



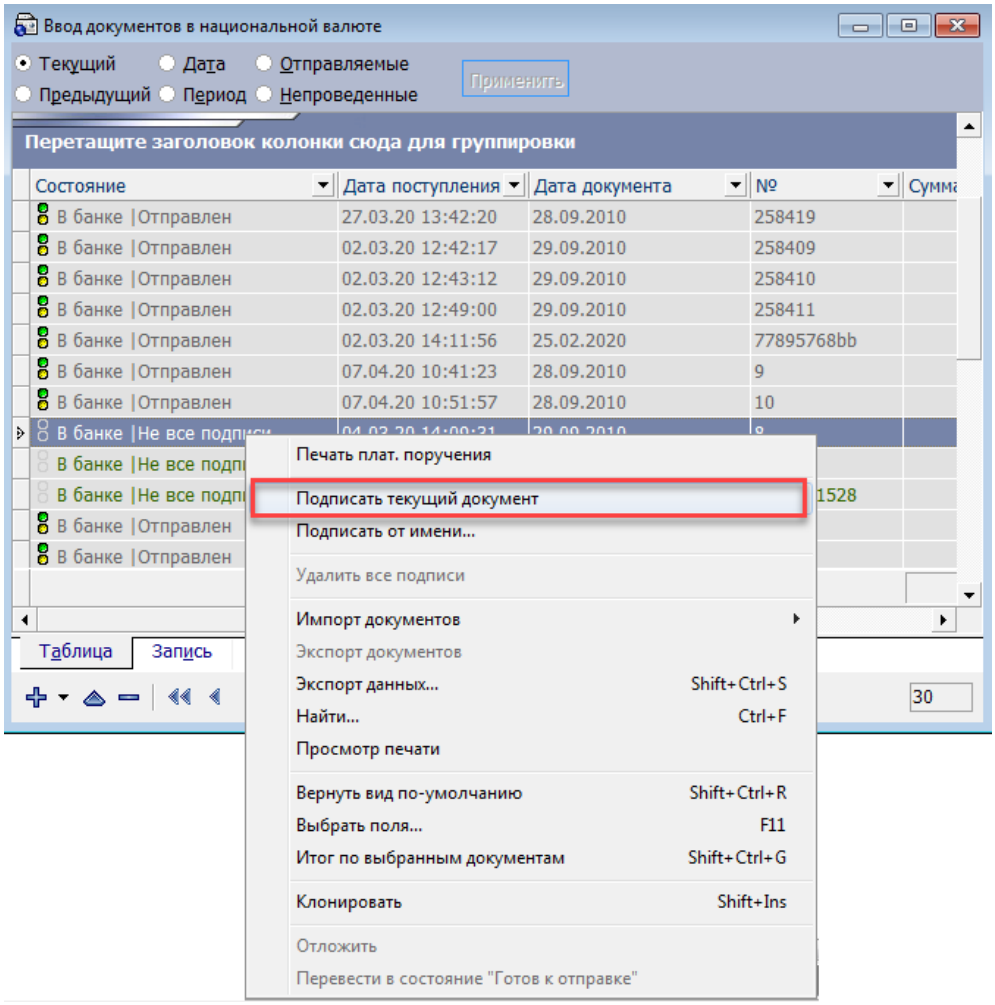
6. После этого вам будет необходимо распечатать и подписать сертификат, заверить его печатью (при необходимости) и предоставить бланк в банк (см. «Просмотр информации о сертификатах»).

3.3. Подписание документов

3.3.1. Наложение электронной цифровой подписи на документ

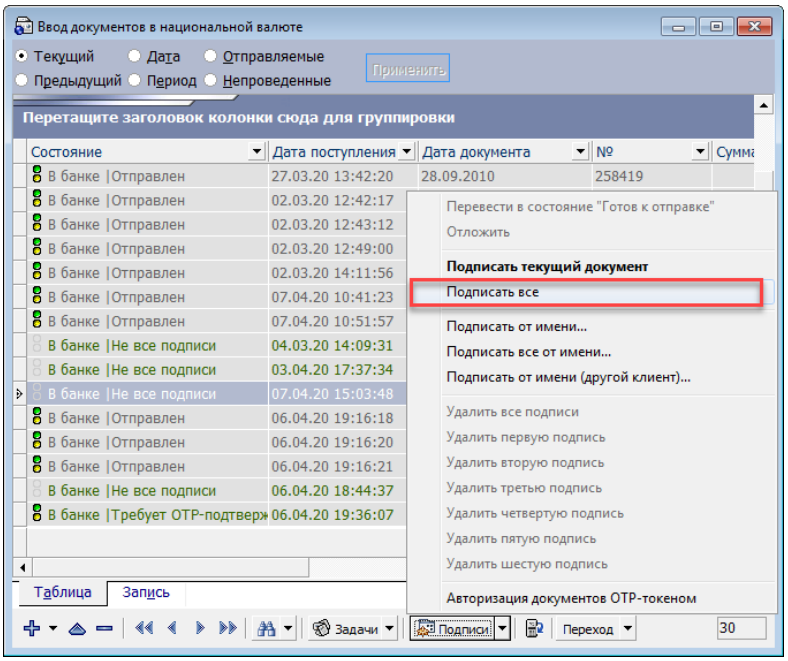
Чтобы наложить свою электронную подпись на документ:

1. Выберите документ, который вы хотите подписать.
2. Вызовите контекстное меню данной записи и выберите операцию ***Подписать текущий документ***. На документ будет наложена ваша электронная подпись (или обе подписи, если у вас есть право накладывать две подписи).



Обратите внимание: пользователь может подписывать документ только при наличии права на соответствующую подпись, а также на дебет счета, с которого будут списываться средства.

Для того чтобы подписать все документы, нажмите кнопку «**Подписи**» в нижней части формы и выберите пункт ***Подписать все***:



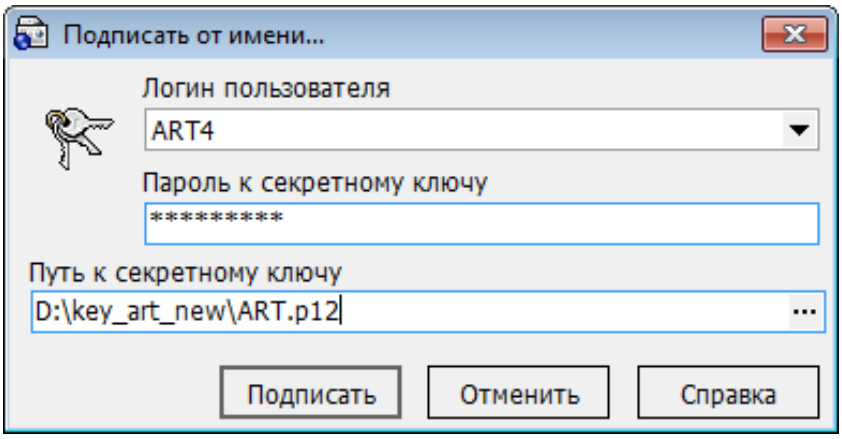
Для отправки документа в банк нажмите кнопку – **«Синхронизировать документы с банком»**.

Обратите внимание: согласно требованиям безопасности, при каждой отправке документа выполняется проверка срока действия и актуальности сертификатов пользователя. Отправляемый в банк документ должен быть подписан только действующими на момент отправки сертификатами. Если же на момент отправки сертификаты какой-либо подписи являются недействительными, система выдаст соответствующее уведомление, а документ будет отправлен с ошибкой.

3.3.2. Подписание документа от имени другого пользователя

Чтобы подписать документ от имени другого пользователя (не того, который подключен к системе в данный момент):

1. Выберите документ, который вы хотите подписать.
2. Нажмите на кнопку , справа от кнопки **«Подписи»** либо вызовите контекстное меню данной записи и выполните операцию ***Подписать от имени***;



3. В открывшейся форме авторизации выберите из выпадающего списка логин пользователя, электронную подпись которого вы хотите наложить на документ.
4. Укажите пароль к секретному ключу.
5. Нажмите кнопку ... и укажите путь к ключу пользователя.
6. Нажмите кнопку **«Подписать»**.
7. Если вы корректно ввели данные пользователя, его электронная подпись будет наложена на выбранный документ.