Система дистанционного обслуживания

для клиентов АБ «УКРГАЗБАНК»

«iTiny»

Version 2.1

Первый вход в систему

ООО “Лайм Системс”

2016

Оглавление

[**1.** **Аутентификация в системе** 3](#_Toc453941177)

[**2.** **Плановая смена пароля** 4](#_Toc453941178)

[**3.** **Важные сообщения** 4](#_Toc453941179)

[**4.** **Создание электронной цифровой подписи** 5](#_Toc453941180)

[**5.** **Смена ПИН на токен** 9](#_Toc453941181)

[**6.** **Подписание электронной цифровой подписью** 10](#_Toc453941182)

[**7**. **Отправка письма от клиента на отделение** 1](#_Toc453941183)2

**Аутентификация в системе**

После того, как банк проведет регистрацию пользователя в системе, на номер, указанный в карточке пользователя, будет отправлено SMS с паролем первого входа, а на заявленный адрес электронной почты будет отправлено сообщение со ссылкой на вход в систему и логином. Запуская систему ИБ <https://itiny.ukrgasbank.com/> откроется стартовая страница, предназначенная для аутентификации пользователя и входа в систему «iTiny». Для входа в систему введите в соответствующие поля **логин** (установленный банком) и **пароль** (SMS сообщение с паролем). Ввод логина и пароля можно выполнить вручную с клавиатуры или для обеспечения дополнительной безопасности воспользоваться кнопкой для вызова экранной клавиатуры, позволяющей ввести логин и пароль. Нажмите кнопку <Войти>.

**ВНИМАНИЕ!** Пароль чувствителен к регистру букв.

**Примечание:** В зависимости от настроек, для аутентификации может быть включена дополнительная защита в виде системы для распознавания символов (CAPTCHA) пользователем.



Рисунок 1 Окно входа в систему

В случае ошибки при вводе логина и/или пароля система выдаст сообщение «Неправильный логин либо пароль!». Проверьте правильность вводимых данных и повторите попытку входа в систему.

После 3-х неудачных попыток входа (количество допустимых попыток может варьироваться в зависимости от настроек системы), доступ будет полностью заблокирован, на определенное время.

Системой может быть предусмотрено подтверждение входа одноразовым паролем, к примеру, через SMS, в таком случае, после проверки корректности введенного логина и пароль, на экране отобразится окно, где будет предложено ввести код подтверждения, а пользователю на телефон придет SMS с кодом.



Рисунок 2 Подтверждение одноразовым паролем

В результате удачного входа в систему на экране отобразится основная страница «iTiny».

**Плановая смена пароля**

При первом входе в систему, пользователь должен сменить временный пароль входа на собственный. В противном случае перемещение пользователя по другим страницам системы будет заблокировано до момента смены пароля.

В открывшемся окне Профиля пользователя, блок *«Смена пароля»*, необходимо ввести пароль первого входа (из SMS) в поле **«Старый пароль»,** после чего заполнить поля **«Новый пароль»** и **«Подтверждение**» паролем, который будет запрашиваться при каждой попытке входа под именем данного клиента. Нажмите кнопку **«Сменить».** Если попытка смены пароля прошла успешно, система выдаст характерное, информационное сообщение. Аналогично, если в момент смены возникнут ошибки, будет показано соответствующее уведомление.



Рисунок 3 Поля для смены пароля

**Примечание**: Пароль первого входа, полученные посредством SMS, имеет ограниченный срок действия, по истечению которого необходимо обратиться в банк для генерации нового.

**Важные сообщения**

После обязательной смены пароля, если банком предусмотрены важные уведомления, система перенаправит вас на страницу с отображением сообщения от банка с пометкой **«Важно».** Такие сообщения являются обязательными к прочтению и блокируют дальнейшую работу с системой. После ознакомления с текстом сообщения, нажмите кнопку **«Пометить как прочитанное».**



Рисунок 4 Сообщение обязательное к прочтению

**Примечание**: В теле важного сообщения могут присутствовать файлы-вложения. Для просмотра вложения, его необходимо загрузить на рабочее место, путем клика мышкой на вложении.

**Создание электронной цифровой подписи**

**ВАЖНО!** Токен должен быть вставлен в USB порт ПК и драйвера к данному устройству корректно установлены.

Ознакомившись со всеми важными сообщениями, если текущий пользователь имеет право первой или второй подписи, система перенаправит к модулю по работе с ключами (ЭЦП). Если автоматическое перенаправление не произошло по какой-либо причине, перейдите, воспользовавшись пунктами меню **«Система» → «Ключи»** либо воспользуйтесь быстрым переходом в верхней левой части экрана, нажав на соответствующую пиктограмму .

Для генерации ключа нажмите 

**Внимание**! Для работы с криптографической системой электронных подписей, необходимо установить и активировать JAVA-applet, используемый для считывания ключей (См. инструкция по JAVA)

**Примечание:** Для начала работы с системой iTiny чтобы пользоваться всеми доступными услугами, включая денежные платежи, переводы средств, оплаты по договорам, клиент должен создать ключ и ждать его сертификации со стороны администратора банка. В системе предусмотрено разделение типов ключей в зависимости от права подписи пользователя (директор / главный бухгалтер), эти подписи называются «Ключ первой подписи» и «Ключ второй подписи».



Рисунок 5 Форма Создания ключа ЭЦП

На экране откроется форма создания ЭЦП, в котором пользователь системы должен:

* Выбрать Тип ключа – Количество связей в выпадающем списке зависит от числа клиентов, к которым привязан пользователь и роль на них (первая/вторая подпись на конкретном клиенте);
* Создать пароль, состоящий из не менее 8-ми символов – Пароль задается для повышения надежности и защищенности ключа ЭЦП. Без знания пароля использование ключа невозможно;
* Ввести пароль повторно;
* Тип устройства «Токен»;

Следующим действием необходимо выбрать путь к токену (рис.6)



*Рисунок 6 Выбор пути к токену*

Получаем окно с выбором токена, где выбираем токен, если их более одного, либо просто подтверждаем выбор «Готово»:





Для завершения генерации ключа с указанным Паролем, нажать кнопку **<Сгенерировать>.**

При запросе ввести ПИН Токена вводим как на рис.7:



*Рисунок 7*

После того как ключ создан, информацию о нем можно просмотреть в окне из меню **«Система**», подменю **«Ключи**». До ожидания сертификации в банке ключ считается не активным и его статус *Регистрация* подсвечивается красным цветом.



Рисунок 8 Информация о ключе

Дальнейшая работа возможна только после процедуры сертификации ключа администратором системы на стороне банка. Поэтому Вам необходимо распечатать и предоставить в банк заявление на сертификацию ключа.

Для вывода на печать сертификата открытого ключа ЭЦП нажмите кнопку **«Заявка на сертификацию»**. Откроется печатная форма сертификата в режиме просмотра. Чтобы распечатать заявление нажмите кнопку «Распечатать>

в верхней части формы просмотра.



Рисунок 9 Печатаная форма сертификата

В ходе активации ключа в банке производится проверка соответствия открытого ключа, находящегося на стороне банка, и секретного ключа, находящегося у клиента (переданного в банк в виде распечатанного заявления). В случае успешной сертификации ключ подсвечивается зеленым и считается активным. Начиная с этого момента и в течение срока действия ключей ЭЦП, Вы можете использовать ключи для отправки платежей и наложения подписи.

При работе с ключами, прежде всего, надо обратить внимание на следующие поля:

|  |  |
| --- | --- |
| [Состояние] | показывает текущее состояние ключа в банке. Отправка платежей возможна только с ключами в состоянии «Активен». |
| [Идентификатор] | уникальный идентификатор открытого ключа. Именно по этому коду выясняется, правильным ли ключом подписан платеж и, соответственно, выполняется проверка соответствия с открытым ключом в банке |
| [Годен до] | показывает дату окончания действия ключа и количество дней до истечения срока годности ключа. Этот параметр необходимо держать под контролем, так как после истечения строка действия ключа, возможность подписывать документы будет утрачена |

Остальные поля являются справочными и могут быть использованы при возникновении проблемных ситуаций.

Для удобства клиента, в системе iTiny реализована функция самоподписи новых ключей, которые были сгенерированы вместо тех, которые утрачивают свою актуальность по истечению срока годности. Для этого, на странице ключей, необходимо нажать кнопку **«Перегенерировать»** в поле нужного ключа, пройти стандартную процедуру создания ключа, после чего необходимо активировать его, нажав **«Сертифицировать»** и подписать старым ключом.

**Смена ПИН на токен**

В случае необходимости смены ПИН на токене вам необходимо проделать следующие действия:

* зайти в меню Система -- > Ключи и нажать 
* нажать на кнопку как на рисунке



* ввести новый ПИН



* нажать на 
* подтвердить предыдущим ПИН-ом, в нашем случае **12345678**



* получаем



**Подписание электронной цифровой подписью**

Подпись, в зависимости от настроек системы, может быть наложена на такие основные:

* Платежи (переводы в национальной валюте);
* Валютные заявки (покупка, продажа, конвертация или перевод валюты);
* Сообщение в банк (информационное сообщение или вложение в нем);
* Ключ (при сертификации самим клиентом).

Для накладывания подписи, необходимо выбрать желаемые элементы, нажать кнопку **«Подписать»**. При осуществлении подписей, на экране откроется окно, в котором система запросит выбрать ключ, которым будет осуществлена подпись, ввести к нему пароль и выбрать место хранения, с указанием пути к ключу.





Рисунок 9 Форма подписи ЭЦП

**Примечание:** Если пользователь имеет более одного типа ключа, либо связь с несколькими клиентами (юр.лицами), в таком случае, системой будет автоматически определена данная связь и выведен определенный перечень ключей для подписания.

Для наложения подписи необходимо:

* Установить флаг  на типе ключа;
* Ввести пароль, установленный при генерации данного ключа (текстовое поле, чувствительное к регистру);
* Выбрать **Тип устройства: Токен** (выпадающий список: файл/токен);
* Нажав кнопку  выбираем токен и подтверждаем кнопкой  (в случаи хранения ключа не на токене указать путь, где хранится ключ (путь указывается до папки, в которой хранится ключ).

Для наложения выбранного типа подписи, нажмите .

Подтверждаем действие введением своего ПИН токена (по умолчанию **12345678**), как на рисунке:



В случае успешной подписи, появится соответствующее уведомление и выбранный объект поменяет свой статус.

Если подписать объект не удалось, система выдаст соответствующее. В данном случае стоит проверить корректность вводимого пароля или наличие вставленного токена в ПК .

**Отправка письма от клиента на отделение**

Необходимо зайти в меню Почта\Новое сообщение выбрать Тему выбрать Тему письма «Листування з відділенням» и выбрать Отделение получателя

І

* написать письмо (вопросы/предложения). После написания письма подтверждаем нажатием кнопки 
* Отметить письмо как показано на рисунке:



* Нажать кнопку 