

Инструкция по использованию одноразовых паролей в системе ДБО АО «Мидзухо Банк (Москва)»

Одноразовые пароли (One-Time passwords – OTP) – динамически генерируемая для единичного использования последовательность символов.

Одноразовые пароли используются для дополнительной аутентификации пользователей системы, которые обладают правом подписи электронных документов. Тем самым обеспечивается дополнительная защита в случае компрометации Логина и Пароля абонента.

Для генерации одноразовых паролей используются специальные устройства – OTP-Токены. В системе дистанционного банковского обслуживания (ДБО) АО «Мидзухо Банк (Москва)» используются автономные генераторы паролей eToken PASS, производства компании Аладдин-РД.



Устройство работает автономно и не требует подключения к компьютеру. Процесс входа в систему ДБО с использованием eToken PASS практически не отличается от обычного – добавлен шаг дополнительной аутентификации с использованием одноразового пароля.

Для выполнения входа в систему необходимо:

1. В адресной строке Internet Explorer набрать адрес сервера системы ДБО <https://online.mhcbr.ru>
2. В появившемся окне

Добро пожаловать в систему ДБО BS-Client v.3!

ВНИМАНИЕ! Для Вашей безопасности рекомендуется использование функционала БЕЗОПАСНОЙ АВТОРИЗАЦИИ

Отключить безопасную авторизацию

Введите Ваши логин и пароль:

Логин

Пароль

ввести персональные Логин и Пароль. Настоятельно рекомендуем вам использовать безопасную авторизацию (ввод учетных данных при помощи экранной клавиатуры). Для этого нажмите кнопку «безопасная авторизация» и в появившемся окне при помощи «мышки» введите ваш Логин и Пароль

3. Вы перейдёте на страницу дополнительной авторизации

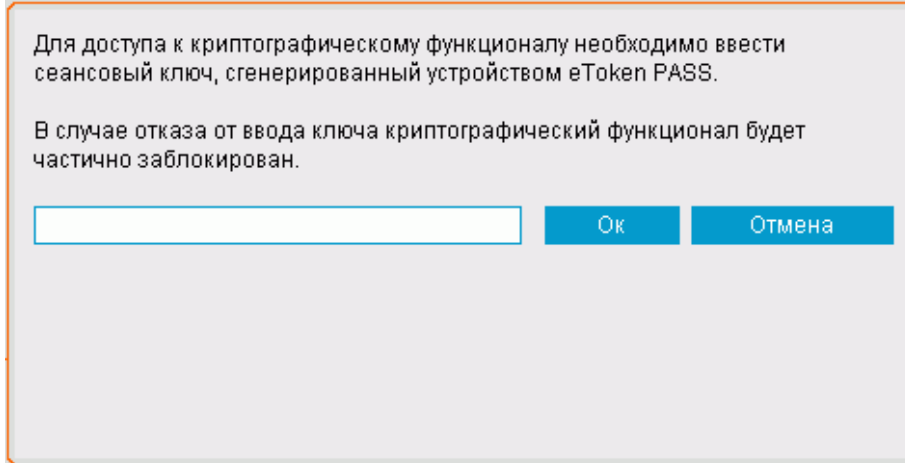
здесь.' (A test communication session will be performed with certificate key verification. You can configure subscriber key parameters [here](#)). A 'Далее' (Next) button is at the bottom right."/>

Выберите пользователя, от имени которого вы входите в систему, и нажмите «далее»

4. Система выдаст следующее сообщение:

Если вы ещё не установили ваш ключевой носитель, установите его и нажмите «далее»

5. Система запросит ввод ключа, сгенерированного устройством eToken Pass:



Для доступа к криптографическому функционалу необходимо ввести сеансовый ключ, сгенерированный устройством eToken PASS.

В случае отказа от ввода ключа криптографический функционал будет частично заблокирован.

Ок Отмена

Для генерации ключа нажмите кнопку на устройстве eToken Pass – сгенерированный ключ отобразится на экране устройства. Введите его в строку ввода и нажмите «Ок»

В результате успешной авторизации система осуществит переход в основной раздел профиля вашей организации. Далее Вы работаете с системой в обычном режиме.

В случае возникновения проблем с использованием устройства eToken PASS просьба обращаться в службу технической поддержки системы ДБО.

Внимание! Категорически запрещается передавать персональный генератор паролей посторонним лицам и генерировать пароли (нажимать на кнопку устройства) вне процесса входа в систему ДБО.