

ПАМЯТКА

по использованию OTP-токена
при подтверждении операций
в системе «iBank 2»



Общие сведения об устройстве OTP-токен

OTP-токен – это компактное и удобное устройство для аутентификации пользователя в системе «iBank 2». Устройство является чрезвычайно простым в работе: при нажатии на функциональную кнопку токен активируется и на LCD-дисплее отображается одноразовый пароль, который необходимо вводить в используемое приложение.

Одноразовый пароль является дополнительным подтверждением на оплату платежных поручений в системе «iBank2».

Данный механизм не заменяет ЭЦП, а является дополнительным подтверждением на оплату платежных поручений. Также может применяться для дополнительной аутентификации Клиента при входе в систему «iBank 2».

OTP-токен обеспечивает гарантированное получение одноразового пароля. Вы можете приобрести OTP-токены в том количестве, в котором это диктуется удобством и порядком работы организации.



Внешний вид OTP-токена
(может различаться в зависимости от модели устройства)

Характеристики устройства и принцип работы

OTP-токен является неразборным, неремонтируемым устройством и не позволяет заменить встроенную батарею. В случае обнаружения на корпусе изделия следов вскрытия или попыток вскрытия пользователь автоматически теряет гарантийные обязательства производителя.

Гарантия на изделие составляет 12 месяцев (с даты продажи). OTP-токен должен эксплуатироваться при температуре окружающего воздуха от +10 до +40 градусов по Цельсию и относительной влажности от 40 до 80 % при температуре 25 градусов по Цельсию.

Срок эксплуатации (время работы встроенной батареи) OTP-токенов составляет 5-7 лет.

Использование OTP-токена в системе «iBank2»

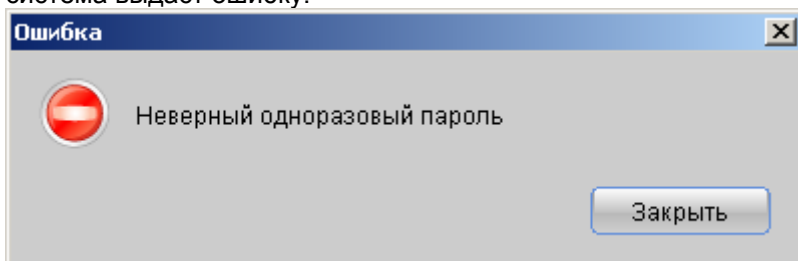
После подписания платежного поручения необходимым количеством ЭЦП, документ переходит в статус «Требуется подтверждение».

Для доставки в Банк такого документа Вам необходимо ввести одноразовый пароль:

Подтверждение одноразовым паролем	
П/п на сумму	99.00 руб.
Получатель	УФК по г.Москве (ФТС России)
БИК	044583001
Счет	40101810400000010153
Способ	OTP-токен
Одноразовый пароль	111111
ОК Отмена	

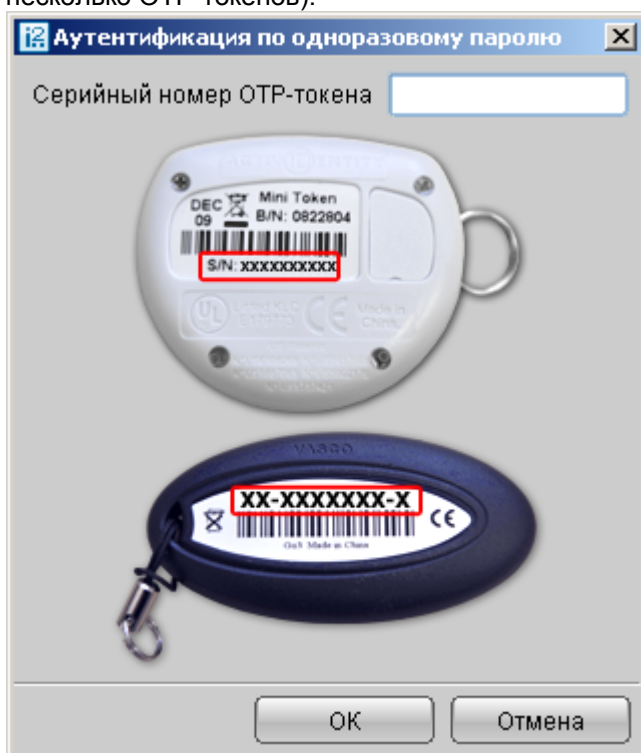
Для получения одноразового пароля необходимо кратковременно нажать кнопку на устройстве. При этом пароль отобразится на LCD-дисплее токена. Через 20 секунд (тайм-аут) в случае отсутствия действий с функциональной кнопкой токен автоматически выключается.

Внимание! Одноразовый пароль необходимо вводить в систему сразу после его появления. Если с момента появления пароля на LCD-дисплее и вводом его в систему пройдет более 60 сек., система выдаст ошибку:



В таком случае необходимо повторить попытку получения одноразового пароля и повторного ввода его в систему.

Если при вводе пароля система выдает сообщение (такое возможно, если у Клиента подключено несколько OTP-токенов):



Вам необходимо указать серийный номер Вашего OTP-токена (его можно посмотреть на обратной стороне устройства, как показано на рисунке).

Подтверждение одноразовым паролем в системе «iBank 2» может быть выполнено как сразу после подписания документа, так и позднее. В РС-Банкинге подтверждение документов выполняется в ходе синхронизации.

Возможно подтверждение отдельного документа или группы документов.

Ключевые реквизиты документов (количество, сумма, реквизиты получателя) отображаются в диалоге подтверждения.

Соблюдение мер безопасности при обращении с OTP-токеном

При обращении с OTP-токеном следует придерживаться следующих рекомендаций:

- запрещено передавать OTP-токен другим лицам;
- хранение OTP-токена должно осуществляться исключительно вне зоны доступности посторонних лиц;
- генерация и использование одноразового пароля должны осуществляться только в момент формирования/проведения платежной операции.

Общие дополнения к правилам безопасности работы в системе «iBank 2»

1. Целесообразно использовать:
 - «USB-токен» для хранения секретных ключей ЭЦП;
 - «SMS-информирование» (сведения: о входе в систему; об изменениях остатков по счетам; об отвержении документа Банком; о поступлении документа; о входящем банковском письме; о движении средств по счету; предоставление текущих остатков по расписанию; получение выписки по расписанию).
2. Соблюдать строгий регламент доступа к рабочему компьютеру системы «iBank 2».
3. Никому не сообщать конфиденциальные сведения (учетные записи и т.п.).
4. Не отвечать на электронные сообщения и запросы с просьбой указать конфиденциальные сведения, не открывать файлы от неизвестных отправителей и пр.
5. Использовать системное и прикладное ПО, полученное из доверенных источников, а также регулярно обновлять указанное ПО.
6. Использовать и регулярно обновлять специализированное ПО для защиты информации – антивирусное ПО, средства защиты от несанкционированного доступа, персональные межсетевые экраны и пр.
7. Соблюдать правила информационной безопасности при работе в Интернете – не посещать подозрительные сайты. Целесообразно выделить отдельное рабочее место к системе «iBank 2» (подключенный только к <https://ibank2.ru>).
8. Не устанавливать программы из непроверенных источников.
9. Незамедлительно информировать Банк обо всех подозрительных ситуациях, инцидентах, внештатных ситуациях и подозрениях на нарушение безопасности рабочего места (заражение компьютера и т.п.).

Внимание!

В случае потери или утраты OTP-токена Вам необходимо незамедлительно обратиться в отделение Банка или связаться с Call-Центром по телефонам: +7 (495) 755 80 08 (для Москвы) и 8 800 100 80 08 (для регионов).