КОНТАКТ-ЦЕНТР

- мобильный номер: 8 (800) 080 07 11 (звонок с мобильного телефона бесплатный);
- городской номер: 8 (7172) 770 622;
- электронная почта: bank@jysanbank.kz;
- время работы: рабочие дни с 8:00 до 22:00

Руководство пользователя СИБ «Jýsan Business»

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ

РЕГИСТРАЦИЯ В СИБ

ДОСТУП В СИБ

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ

Требования безопасности СИБ

Клиенту необходимо соблюдать требования и рекомендации безопасности для исключения риска несанкционированного доступа к счету, получения информации по счету и инициирования платежных документов.

Общие требования и рекомендации безопасности

1. Для платежных документов и, особенно, для документов на большие суммы, использовать несколько уровней подписи документов; при этом использование карт OTP для подписи платежных документов на большие суммы является предпочтительным по отношению к SMS OTP; уровень критичности сумм определяется Клиентами самостоятельно;
2. не сообщать данные (ПИН-коды, статические пароли, пароли к электронной почте) по доступу к СИБ третьим лицам, включая работников Банка;
3. при доступе к электронной почте для получения OTP, защищать потовый ящик сложным паролем при использовании прописных и строчных букв, цифр и спецсимволов, при длине пароля не менее 8 символов;
4. не передавать физические устройства (мобильные телефоны, карты OTP) для доступа к СИБ третьим лицам, включая работников Банка;
5. не оставлять физические устройства (мобильные телефоны, карты OTP) для доступа к СИБ в открытом доступе;
6. при утере физических устройств (мобильные телефоны, карты OTP) для доступа к СИБ, незамедлительно связаться с Банком для блокирования доступа к СИБ; убедиться, что по счетам не были проведены несанкционированные платежи;
7. при подозрении на компрометацию данных (ПИН-коды, статические пароли, пароли к электронной почте) по доступу к СИБ, незамедлительно изменить данные; убедиться, что по счетам не были проведены несанкционированные платежи.

Использование статических паролей к МП, web версии СИБ и электронной почте

1. Рекомендуется менять пароли не реже одного раза в месяц;
2. не сообщать пароли третьим лицам, при подозрении на компрометацию незамедлительно изменить пароли;
3. не хранить пароли в кэш временных файлов устройства; при случайном сохранении паролей, чистить кэш;
4. при доступе к СИБ с мобильного устройства с привязанной к устройству электронной почтой, не хранить пароли в кэш временных файлов устройства; при каждом доступе к электронной почте с мобильного устройства, вручную вводить пароли без сохранения в кэш.

Использование мобильного устройства с установленной мобильной версией

1. Не оставлять мобильное устройство в открытом доступе;
2. не передавать мобильное устройство третьим лицам;
3. защищать мобильное устройство при использовании биометрии (отпечаток пальца, слепок лица) или ПИН кода; использование биометрии предпочтительно;
4. при получении OTP по SMS и email на одном устройстве необходимо разделять каналы получения, защищая доступ к email сложным паролем при использовании прописных и строчных букв, цифр и спецсимволов, при длине пароля не менее 8 символов;
5. не хранить пароли в кэш временных файлов устройства; при случайном сохранении паролей чистить кэш;
6. при подозрении на компрометацию данных (ПИН-код на устройстве, пароли) незамедлительно изменить данные.

Использование web версии СИБ на стационарных устройствах

1. Не оставлять компьютер с запущенной активной сессией СИБ без присмотра, при покидании рабочего места блокировать компьютер;
2. не хранить пароли СИБ в кэш временных файлов устройства; при случайном сохранении паролей чистить кэш;
3. при подозрении на компрометацию данных (пароли к СИБ, электронной почте) незамедлительно изменить данные;
4. при доступе с компьютера к электронной почте для получения OTP защищать потовый ящик сложным паролем с использованием прописных и строчных букв, цифр и спецсимволов, при длине пароля не менее 8 символов.

ПРОЦЕДУРЫ БЕЗОПАСНОСТИ

Карта OTP в web-версии

- Карта используется для подписи платежных документов в СИБ;
- карта представляет собой пластиковую форму с клавиатурой для ввода ПИН-кода (4 цифры) и LCD дисплеем, отображающим единовременные пароли OTP (6 цифр) для ввода в СИБ и питается от встроенного аккумулятора;
- пароль OTP действителен 30 секунд, после чего карта формирует новый пароль;
- срок службы карт OTP составляет до 5 лет в зависимости от частоты их использования и условий хранения.

Требования безопасности

1. При получении из Банка новой карты OTP незамедлительно установить ПИН-код к ней;
2. не сообщать ПИН-код третьим лицам, включая работников Банка;
3. хранить карту OTP в месте, недоступном для третьих лиц;
4. рекомендуется менять ПИН-код не реже одного раза в месяц;
5. при подозрении на компрометацию ПИН-кода незамедлительно изменить его согласно инструкции по работе с картой OTP, размещенной на сайте Банка; убедиться, что по счетам не были проведены несанкционированные платежи;
6. не передавать карту OTP третьим лицам, включая работников Банка;
7. не оставлять карту OTP в открытом доступе;
8. при утере карты OTP незамедлительно связаться с Банком для временного блокирования доступа с последующей заменой карты OTP на новую;
9. при наличии платежных документов на большие суммы использовать метод подписи при использовании карт OTP, как предпочтительный по отношению к SMS OTP.

Установка нового ПИН-кода к карте

1. Включите карту, нажав «OK», карта сообщит «No1» и затем «----»;
2. введите новый ПИН-код (4 цифры) и нажмите «OK», карта сообщит «No2»;
3. повторно введите новый ПИН-код и нажмите «OK», карта сообщит «SUCCES» и затем «-»;
4. нажмите «OK» для выключения карты, в дальнейшем используйте новый ПИН-код.

При неверном изменении ПИН-кода, карта сообщит «Err». Выключите карту, нажав «OK» и повторите установку нового ПИН-кода.

Сообщения карты при неверном вводе ПИН-кода:

- «Err1» – введен неверный ПИН-код;
- «Err2» – дважды введен ошибочный ПИН-код;
- «Err3» – трижды введен неверный ПИН-код;
- «Lock» – карта временно заблокирована в связи с вводом ошибочного ПИН-кода.

Разблокирование карты

Если трижды ввели неверный ПИН-код, карта временно блокируется и требует разблокирования:

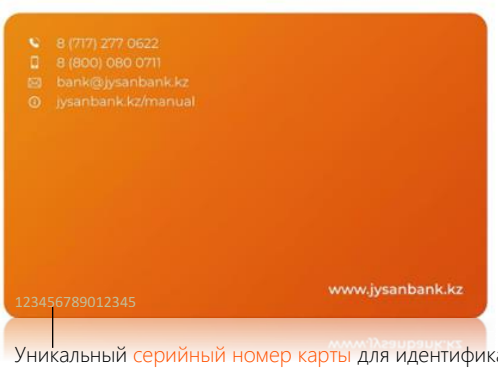
1. Включите карту, нажав «OK», на LCD дисплее карты отобразится PUK-код 6 (цифр);
2. свяжитесь с менеджером контакт-центра Банка и сообщите ему PUK-код;
3. полученный от менеджера код разблокирования введите в карту;
4. карта сообщит «No1»; придумайте новый ПИН-код, введите его в карту и нажмите «OK»;
5. карта сообщит «No2»; повторите новый ПИН-код и «OK»;
6. карта сообщит «SUCCES», что означает успешную смену ПИН-кода.

Многофункциональная кнопка OK для ввода ПИН-кода, смены ПИН-кода и пр.

LCD дисплей для отображения информации (пароли, сообщения карты)

Клавиатура для ввода данных в карту

Кнопка включения и выключения карты, удаления последнего введенного в карту символа и пр.



Уникальный серийный номер карты для идентификации пользователя при подписи документов в СИБ

РЕГИСТРАЦИЯ В СИБ

Регистрация в приложении

Регистрация пользователей в СИБ осуществляется пользователями самостоятельно, удаленно с web и мобильных устройств. При регистрации используются два фактора авторизации - доверенный номер телефона и электронный адрес.

Для каждого регистрирующегося в СИБ пользователя, в Банке предварительно должны быть зарегистрированы следующие данные:

- Подтверждённый доверенный номер мобильного телефона пользователя;
- электронный почтовый адрес;
- роль в СИБ (руководитель с правом первой подписи, бухгалтер с правом второй подписи, доверенное лицо без права подписи).

Идентификатор клиента и номер телефона

Уникальным идентификатором клиента является его ИИН, логином клиента является его номер телефона.
Для корректной идентификации клиента и подвязки его счетов система использует связку ИИН + логин (номер телефона). Единственным способом подвязки номера телефона (или его обновления) является обращение к менеджеру.

Процесс регистрации

1. Пользователь вводит доверенный номер телефона. При этом имеет возможность исправить номер телефона и нажать «Далее».
2. Пользователь вводит код из SMS:
   - SMS правильный.
   - Введенный SMS-код неверный. У пользователя есть 5 попыток на каждый SMS-код. В случае 5 неправильных вводов предлагается отправить новый код. Это возможно сделать только через минуту после запроса первого кода.
   - Истек срок жизни SMS-кода (1 минута). Пользователю доступна кнопка “Отправить повторно” по истечению 1 минуты после отправки последней SMS.
   - Пользователю отображается текст: "Не получили SMS?". По истечении 1 минуты с момента отправки счетчик подменяется ссылкой на повторную отправку.
3. При правильном коде из SMS система направляет Пользователя на следующий шаг (подтверждение через email адрес) и автоматически отправляет OTP-код на email адрес, указанный в карточке клиента. При этом на экране Пользователю отображаются маскированный адрес и сообщение: "Пожалуйста, введите код подтверждения, который мы выслали на ваш email адрес".
   Если Пользователь нажмет кнопку «Назад», то его возвращает на экран ввода номера телефона.
   - Код подтверждения из почты правильный - см. п. 5
   - Код подтверждения неверный. У Пользователя есть 5 попыток на каждый код. В случае 5 неправильных вводов Пользователю предлагается отправить новый код. Это возможно сделать только через минуту после запроса первого кода.
   - Истек срок жизни кода подтверждения (5 минут). Пользователю доступна кнопка “Отправить повторно”.
   - Пользователю отображается текст: "Не получили код на email?" и счетчик времени для повторной отправки. По истечении 1 минуты с момента отправки, счетчик подменяется ссылкой на повторную отправку. Пользователь возвращается на экран ввода номера телефона и нажимает кнопку «Далее» с этим же номером телефона.
4. При успешном подтверждении кода из email Пользователю предлагается установить пароль для входа.
5. Пользователь вводит пароль дважды (система проверяет точное совпадение).
6. При любом прерывании жизни приложения на смартфоне до этого шага Система сбрасывает процесс, Пользователю необходимо выполнить процедуру с первого шага. При успешном создании пароля система регистрирует Пользователя в СИБ и сразу авторизует его в системе.
7. При регистрации с мобильного устройства система так же просит Пользователя в обязательном порядке установить ПИН- код быстрого доступа.
8. После успешной установки ПИН-кода система предлагает опционально подключить авторизацию посредством биометрии (нативные Face ID/Touch ID).
9. Также при первичной успешной регистрации проходит процесс запоминания устройства клиента (смартфона или стационарного компьютера).

ДОСТУП В СИБ

Вход в приложение

1. Вход возможно осуществлять с web и мобильных устройств по адресу https://ib.jysan.kz
2. В качестве логина используется номер телефона Пользователя и пароль, который Пользователь устанавливает при регистрации.
3. Система всегда запрашивает Device Token при логине. Если его нет, помимо авторизации по логину и паролю, происходит дополнительная авторизация посредством SMS OTP.

Web-авторизация

1. Для web-авторизации возможно использовать несколько одновременных сессий и доступы с нескольких устройств.
2. При успешном входе по номеру телефона и паролю, происходит авторизация Пользователя. При доступе с нового устройства происходит SMS-авторизация Пользователя по аналогии с процессом Регистрации. При успешном SMS-подтверждении, система запоминает устройство Пользователя.
3. При доступе с незарегистрированного номера телефона, система сообщает «Данный номер телефона не зарегистрирован. Вам необходимо пройти регистрацию».
4. После 10 неправильных вводов пароля Пользователь блокируется на 1 час. При этом отображается сообщение "Вы превысили количество попыток авторизации. Попробуйте авторизоваться позже." Настройки Пользователя СИБ в телефоне удаляются.
5. Для мобильных устройств возможна авторизация только на одном устройстве. При авторизации с другого устройства сбрасывается ПИН-код и стираются настройки Пользователя.

Использование ПИН-кода

Если у Пользователя на устройстве установлена нативная биометрия, система авторизует Пользователя в соответствии с нативными требованиями.

При 5 неуспешных попытках исключается возможность авторизации по биометрии.
При успешном вводе пасс-кода, система авторизует Пользователя.
При неуспешном вводе пасс-кода система включает счетчик и отображает Пользователю количество попыток. При 5 неуспешных попытках система сбрасывает экран пасс-кода и удаляет настройки Пользователя на устройстве.
Пользователю доступна кнопка «Выход» на экране ввода пасс-кода. При нажатии на нее в системном окне отображается сообщение «Вы уверены, что хотите выйти? Вход потребует ввода пароля», опции «Выйти» (красным цветом) и «Отмена». При выходе система сбрасывает ПИН-код и удаляет пользовательские настройки.

Использование статического пароля

Система предлагает авторизоваться посредством статического пароля так же как при web.
При успешной авторизации система требует создать ПИН-код и запоминает Пользователя на устройстве.

Восстановление доступа

В web и мобильных приложениях система дает возможность восстановить доступ к учетной записи Пользователя. Для этого Пользователю на экране логина отображается ссылка «Забыли пароль?», при нажатии на которую запускается процесс регистрации Пользователя.
Система в точности повторяет процесс регистрации.
При успешном завершении у Пользователя обновляется пароль к учётной записи, стираются настройки, кроме заново созданных по результатам процедуры восстановления.