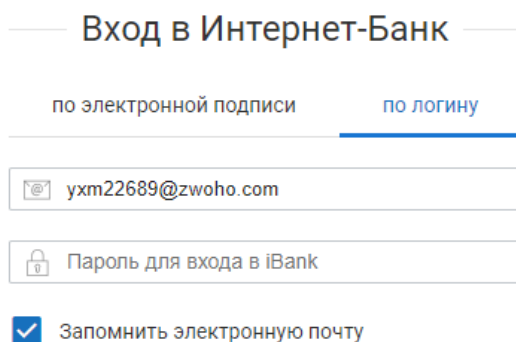


## «ЧЕЛИНДБАНК-БИЗНЕС»

### Одна точка входа для работы с группой связанных предприятий, находящихся под единым контролем или управлением, с использованием технологии «Вход по логину»

Достаточно распространенной ситуацией в бизнесе является работа группы связанных предприятий, находящихся под единым контролем или управлением, а также передача ведения бухгалтерии организации на аутсорсинг. Ключи, расположенные на аппаратных устройствах USB-токен, позволяют уполномоченному сотруднику работать с несколькими предприятиями, каждый раз заново заходя для выполнения операций в другом предприятии. При этом нужно выйти из текущего предприятия, выбрать другой ключ, ввести к нему пароль, получить одноразовый код по SMS и лишь потом начать работу с новым предприятием.

Новая технология «Вход по логину», предлагаемая ПАО «ЧЕЛИНДБАНК» своим клиентам, позволяет работать со связанной группой предприятий (далее – пул) более комфортно.



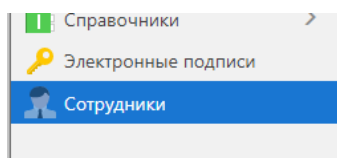
Для перехода к технологии «Вход по логину» клиенту необходимо создать учетные записи интернет-банка в настройках своих предприятий. При этом клиент может продолжать использовать существующие ключи, хранящиеся на аппаратных устройствах USB-токен для подписи документов, но имеет право создать ключи облачной подписи для повышения мобильности доступа.

Для предприятий, уже подключившихся к «Челиндбанк-Бизнес» с облачной подписью, но не использовавших технологию единого логина для объединения в пул, можно сделать это, приведя логины всех предприятий к единому.

**Главное правило объединения в пул: «Сотрудник видит в едином пуле все предприятия, в которых для него создана одинаковая учетная запись (email + телефон)».**

### Создание логина и использование существующих ключей на USB-токенах

В этом случае клиент не меняет привычный способ подписи документов, используя логин исключительно для объединения предприятий в пул. Но нужно понимать, что ключи связаны с конкретным сотрудником, к которому и нужно будет привязать ключ с правом подписи.



В разделе «Сотрудники», который доступен сотрудникам с ролью «Руководитель организации» или «Администратор», необходимо найти нужного сотрудника и открыть его карточку.

Шангин Сергей Геннадьевич

Личные данные    Учетные записи    ЭП и средства подтверждения    Права

Фамилия: Шангин  
Имя: Сергей  
Отчество: Геннадьевич  
Должность:   
 Руководитель

Так как у сотрудника нет «Учетной записи», необходимо ее назначить, указав email и телефон в разделе «Интернет-банк (вход по логину)». Для перехода к вводу данных нажмите кнопку «Добавить»:

Личные данные    Учетные записи    ЭП и средства подтверждения    Права

**Интернет-Банк (вход по логину)**

---

Личные данные    Учетные записи    ЭП и средства подтверждения    Права

**Интернет-Банк (вход по логину)**  
Логин (E-mail)  
Мобильный телефон

На указанный при регистрации учетной записи email будет отправлено письмо для завершения регистрации – вам необходимо задать пароль для входа. Требования к паролю указываются, вам необходимо им следовать для создания безопасного пароля. Учетная запись будет привязана к тому сотруднику, для которого она создавалась. Если у этого сотрудника есть действующий ключ, хранящийся на токене, он сможет использовать его при подписании документов.

При первом предъявлении ключа, хранящегося на токене, необходимо ввести пароль доступа к ключу. В дальнейшем, в рамках текущего сеанса работы, пароль запрашиваться не будет. При переходе к другому предприятию будет запрашиваться ключ, связанный с выбранным предприятием. Система в целях безопасности сбрасывает данные о запомненном на время сеанса пароле, при переходе к другому предприятию.

**Примечание:** Один из сотрудников клиента, обычно это директор, имеет роль «Руководитель организации», позволяющую ему управлять своими сотрудниками и ключами. Одна из функций управления – наделение сотрудника ролью «Администратор». Администратор имеет равное с руководителем право управления сотрудниками, то есть руководитель может делегировать свои функции управления любому другому сотруднику по своему желанию.

### Использование облачных подписей (мобильность)

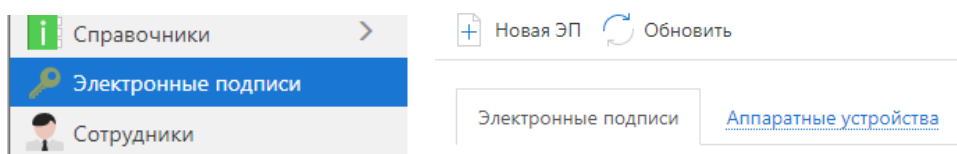
Так как ключ, хранящийся на USB-токене, физически связан с носителем, возникают проблемы мобильности. Обычно носители хранятся в сейфе уполномоченного лица и не позволяют другому лицу или самому уполномоченному подписать документ, оказавшись неожиданно вдалеке от сейфа.

Можно, конечно, заблаговременно озаботиться и взять USB-токен с собой в поездку, но это не очень безопасно, возможен выход носителя из строя по любой причине и, как следствие, в нужный момент у клиента под рукой не окажется электронной подписи.

Альтернативный вариант – использование ключа облачной электронной подписи (далее – ключ ОЭП), хранящегося на серверах банка, не имеющего физического хранилища, доступного в любой момент из любой точки мира, где в данный момент оказался уполномоченный сотрудник. Этот ключ не может «сломаться», он доступен по первому требованию, для его использования сотруднику нужно лишь войти под правильным логином (email + пароль, одноразовый пароль на телефон, связанный с логином) и знать пароль от облачного ключа, который будет вызван из облачного хранилища при необходимости подписи. Не имея что-то из вышеуказанного, никто не сможет выполнить критически важное действие – списать деньги со счета клиента.

Облачная подпись неразрывно связана с понятием логина, данные вводятся на этапе создания ключа ОЭП.

Для клиента, уже работающего в системе iBank2, процедура создания ключа и логина начинается также в его личном кабинете, но в разделе «Электронные подписи».



Клиент выбирает «+ Новая ЭП» и выбирает сотрудника, для которого необходимо создать ключ. Выбираем и нажимаем «Вперед» – открывается карточка сотрудника:

Получение новой ЭП

Укажите сведения о себе

Фамилия	Шангин		
Имя	Сергей		
Отчество	Геннадьевич		
Должность	Тестер		

Документ, удостоверяющий личность.

Тип	Паспорт гражданина РФ		
Серия	3333	Номер	333333
Дата выдачи	03.03.2003	Код подразделения	333-333
Кем выдан	УВД г. Челябинска		

Назад Вперед

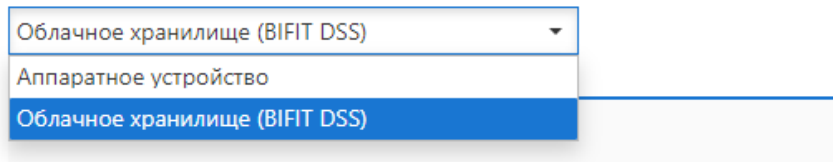
Если данные верны, нажимаем «Далее» и выбираем тип хранилища «Облачное хранилище (Bifit DSS)»

### Выберите место хранения ключа электронной подписи

**Электронная подпись должна быть добавлена в хранилище.**

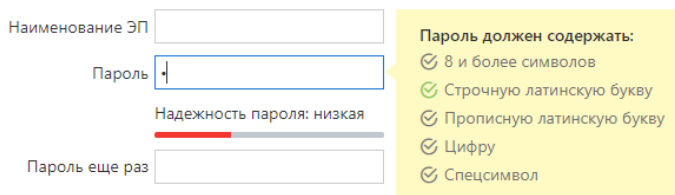
В одном хранилище может содержаться несколько ключей ЭП.

Если хранилище не существует, будет создано новое.



На следующем шаге необходимо указать наименование ключа – определение, позволяющее однозначно понять, какой именно ключ будет вам предложен. Обычно это краткое название предприятия и некая дополнительная информация (Иванов И.И., директор, гл.бух. и т.п.).

Пароль для ключа должен отвечать требованиям безопасности, по мере того, как введенные вами символы и их количество удовлетворяют указанным требованиям, будут загораться зеленые галочки:



Не используйте технологию «русскими буквами в английской раскладке», потому что это не позволит вам ввести пароль на сенсорной клавиатуре мобильного устройства. Облачный ключ используется равноправно в web- и в мобильном приложениях.

Подтвердите пароль и постарайтесь сделать все необходимое, чтобы он не забылся – не используйте визуально похожие символы – заглавная буква «О» и ноль «0», которые в записи легко перепутать; плохая идея использовать в качестве спецсимвола точку, она может потеряться в записи на бумаге. Если есть необходимость, запишите пароль в надежном месте, чтобы обратиться к заметкам в случае форс-мажора.

На следующем шаге вам предложат проверить данные и сохранить заявление на выпуск ключа ОЭП. Если данные верны, сохраните результаты работы – будет создано заявление на выпуск ключа ЭП. Сохраните и подпишите его действующей подписью, хранящейся на токене – заявление уйдет в банк и ваш ключ будет активирован банком без необходимости посещения офиса банка.

Как только на почту, указанную при создании ключа, придет письмо о необходимости завершения регистрации, следуйте инструкции после нажатия на кнопку «Закончить настройку». Помните, что пароль для входа (логина) и ключа может различаться, но в вашей власти сделать их одинаковыми, чтобы уменьшить количество хранящейся в памяти информации.

## iBank для Бизнеса

Шангин Сергей Геннадьевич

Вам предоставлен доступ по логину и паролю в систему "iBank для Бизнеса" банка ПАО "ЧЕЛИНДБАНК".

Осталось [закончить настройку](#) входа.

Организация

ООО НПО "Урал"

ИНН

7449064570

[Закончить настройку](#)

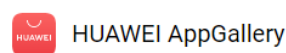
Ссылка действительна до 20.01.2021 14:52

Для каждого предприятия, входящего в группу, необходимо создать собственный ключ ОЭП, указывая единый логин для каждой генерации. Письмо, приходящее после активации ключа на стороне банка, не будет требовать от вас создания пароля для входа по логину, так как логин был уже активирован, но формально будет подтвержден ваш телефон.

### Подключение мобильного приложения (информационный)

ПАО «ЧЕЛИНДБАНК» предлагает своим клиентам удобный сервис – мобильное приложение «Челиндбанк-Бизнес». Приложение предоставляется бесплатно, за его использование не взимается абонентская плата. Приложение может работать в двух режимах: информационный (просмотр выписок и писем) и базовый (создание платежных документов и писем, подпись документов). Приложение не допускает анонимной регистрации, но режим информационный клиент может подключить самостоятельно.

В своем личном кабинете web-системы «Челиндбанк-Бизнес» в разделе «Сотрудники» - «Учетные записи» в любой момент для любого сотрудника можно создать учетную запись для мобильного приложения, указав номер телефона, на котором оно будет установлено. При этом доступ будет в информационном режиме, то есть клиент сможет просматривать выписки и письма. Если этого достаточно, то, закончив создание учетной записи для мобильного банка, можно устанавливать собственно мобильное приложение из соответствующего магазина приложений. Мобильное приложение «Челиндбанк-Бизнес» в магазинах приложений Google Play, Apple App Store и Huawei AppGallery:



*Обратите внимание, что мобильное приложение «Челиндбанк» – это мобильный банк для физических лиц.*