

Правила доступа клиентов к услугам ДБО РосБизнесБанк.

Между клиентом и АРКБ РосБизнесБанк (ПАО) заключается договор об использовании электронных документов в расчетах, содержащий в том числе положения, регламентирующие механизм решения конфликтных ситуаций, использование сертифицированных ФСБ систем электронной подписи и шифрования, а также порядок ввода в действие и применение ключей электронной подписи и шифрования.

Доступ клиентов осуществляется через информационно-телекоммуникационную сеть «Интернет». Клиент, из любой точки мира, при помощи web-браузера Google Chrome, Internet Explorer обращается по протоколу HTTP к web-серверу ДБО РосБизнесБанк.

Аутентификация соединения осуществляется по протоколу SSL или TLS. При успешной аутентификации соединения клиент проходит процедуру многофакторной аутентификации в системе, после чего, в случае положительного результата, начинает защищенный сеанс работы с системой «Интернет-Клиент» - производится обмен информацией в форматах HTML и XML. Клиент может создавать и редактировать распоряжения на осуществление перевода денежных средств и иные документы, просматривать архив документов, сообщения из ДБО РосБизнесБанк и выписки по банковскому счету за любой период, пользоваться справочной информацией, находящейся на стороне АРКБ РосБизнесБанк (ПАО).

При подготовке любого документа осуществляется его контроль на корректность введенных данных, после чего осуществляется операция создания электронной подписи. Далее документ отправляется на обработку и после проведения процедур приема к исполнению попадает в общую базу данных единой банковской части «АБС БИС», где производится его дальнейшая обработка. При выполнении обработки документа, клиент получает подтверждение исполнения документа или уведомление об отказе в выполнении распоряжения с указанием причины.

Так же просим обратить внимание на следующие пункты.

- Внимательно читайте SMS-сообщения, всегда проверяйте реквизиты операции. Если Вам пришло сообщение с операцией, которую Вы не совершали, ни при каких обстоятельствах не вводите пароль.
- Не сохраняйте пароль к системе ДБО в памяти Интернет браузера.
- Используйте только лицензионное антивирусное ПО с постоянно обновляемыми базами.
- При смене номера телефона, на который подключено СМС-уведомление, Вам необходимо обратиться в любое отделение банка и оформить заявление на «смену номера телефона» для SMS-сообщений .
- Если к вам обратились по телефону, в интернете, через социальные сети или другими способами, и под различными предложениями пытаются узнать данные о вашей банковской карте, пароли или другую персональную информацию, будьте осторожны: это явные признаки мошенничества. При любых сомнениях рекомендуем прекратить общение и обратиться в банк по телефону, указанному на обратной стороне вашей банковской карты или на WEB сайте банка.