

Безопасность использования Интернет-банка FinOnline

Для доступа к Интернет-банку FinOnline (далее – Интернет-банк) необходим персональный компьютер или мобильное устройство, подключенное к сети Интернет.

Авторизация

Клиент вводит Аутентификационные данные каждый раз при входе в Интернет-банк. При отсутствии активных действий Клиента в Интернет-банке через определенное время сессия автоматически заканчивается. Для продолжения работы в Интернет-банке пользователю необходимо заново ввести Аутентификационные данные. Клиент обязан исключить доступ третьих лиц к Аутентификационным данным.

Шифрование данных

Интернет-банк использует систему шифрования данных. Так как Интернет-банк использует для связи Клиента и Банка сеть Интернет, во избежание случаев стороннего вмешательства в конфиденциальную информацию Клиента, информация шифруется и в зашифрованном виде передается от Клиента к Банку и обратно.

Обеспечение безопасности соединения в сети Интернет

Интернет-банк имеет всегда один адрес - www.fin-online.ru

Клиент должен всегда собственноручно набирать в адресной строке браузера адрес Интернет-банка www.fin-online.ru либо переходить по ссылке, размещенной на официальном сайте Банка www.finsb.ru. Запрещается переходить на сайт Интернет-банка по ссылкам, размещенным в электронных письмах или на сайтах в сети Интернет (кроме официального сайта Банка).

После входа на стартовую страницу необходимо удостовериться, что соединение установлено по протоколу HTTPS, т.е. в адресной строке указано: <https://www.fin-online.ru/> и в наличии значка защищенного соединения – замочка – в правом нижнем углу или в адресной строке браузера.



Сертификат безопасности, который можно посмотреть при двойном нажатии на этот значок, должен быть выдан Thawte SSL CA. для сайта www.fin-online.ru

Клиент должен обеспечить безопасность персонального компьютера или мобильного устройства, с которого осуществляется доступ в Интернет-банк, в т.ч.:

- допускать к персональному компьютеру или мобильному устройству только доверенных лиц, за действия которых Клиент отвечает как за свои собственные;
- использовать на персональном компьютере или мобильном устройстве только лицензионное программное обеспечение;
- использовать персональный компьютер или мобильное устройство, на котором установлена только одна операционная система;
- работать в операционной системе персонального компьютера под локальной учетной записью с ограниченными правами доступа. На мобильных устройствах не использовать модифицированные или измененные операционные системы;
- установить на персональном компьютере специальные программные и аппаратные средства защиты (межсетевые экраны (firewall), антивирусное программное обеспечение, средства обнаружения вредоносных кодов), которые должны регулярно обновляться;
- производить регулярное обновление программного обеспечения, установленного на персональном компьютере и мобильном устройстве;
- запускать на персональном компьютере и мобильном устройстве программы, полученные только из доверенных источников (особую опасность могут представлять программы, полученные по электронной почте или из сети Интернет); файлы, полученные из общедоступных сетей передачи данных, не рекомендуется открывать и использовать без проведения соответствующих проверок для исключения программных закладок и вирусов;
- установить парольную защиту на вход в персональный компьютер и мобильное устройство.

Система переписки с Банком

Банк никогда не будет посылать письмо или звонить Клиенту по телефону, с просьбой сообщить Аутентификационные данные, а также любую другую личную информацию Клиента.

Блокировка доступа

В случае трехкратного неправильного ввода SMS-кода доступ Клиента в Интернет-банк будет автоматически заблокирован. Это делается с целью предотвращения подбора клиентского SMS-кода злоумышленниками (путем перебора возможных вариантов). Для разблокировки доступа Клиент должен обратиться в Банк телефону (495) 777-6-777 (для звонков по Москве) или 8-800-2000-767 (бесплатный звонок по России)