

Рекомендации по информационной безопасности при работе в Системе ДБО.

1. Общие положения.

1.1. Использование средств дистанционного банковского обслуживания всегда связано с повышенными рисками, поэтому ознакомьтесь с настоящими Рекомендациями до начала работы в Системе ДБО.

1.2. При работе в Системе используются следующие средства защиты:

1.2.1. Защищенное соединение с Банком.

- Признаком установки защищённого соединения является наличие информации о протоколе `https` в адресной строке используемого клиентом браузера (<https://elf.faktura.ru/elf/app/?site=maritimebank>).
- При входе в Систему ДБО всегда проверяйте указанный адрес.

1.2.2. Виртуальная клавиатура.

- Виртуальная клавиатура повышает степень защищенности Вашего пароля от перехвата злоумышленниками.
- Виртуальная клавиатура появляется при входе в Систему ДБО.
- При входе в Систему наберите Ваш Логин на обычной клавиатуре. Затем для ввода Пароля используйте виртуальную клавиатуру: при помощи указателя мыши введите на виртуальной клавиатуре пароль доступа к Системе ДБО (если пароль содержит заглавную букву или символ, нажмите клавишу `Shift`, переключение между русским и английским алфавитом – клавиша `Рус/Lat`, для удаления предыдущего символа используется стрелочка), по окончании ввода пароля нажмите `Enter`.

1.2.3. Средства подтверждения.

- Одноразовые пароли используются при входе в Систему ДБО и проведении операций в Системе ДБО. Одноразовые пароли направляются sms - сообщением на Ваш телефон, указанный в Заявлении о присоединении к Договору.
- После ввода Логина и Пароля для входа в Систему ДБО, Система ДБО потребует ввести Одноразовый пароль.
- После ввода всех данных для перевода денежных средств Система ДБО предложит ввести Одноразовый пароль с целью подтверждения операции.
- Одноразовый пароль должен быть введен Вами в течение 360 секунд. Если в течение указанного времени Одноразовый пароль не был введен, он становится недействительным. В этом случае на Ваш телефон будет направлено новое sms - сообщение с новым Одноразовым паролем.

2. Требования информационной безопасности при работе в Системе ДБО.

2.1. Используйте только лицензионную операционную систему на Вашем компьютере.

2.2. Своевременно устанавливайте обновления операционной системы и прикладных программ, рекомендуемые разработчиком программного обеспечения. Копируйте обновления только с официальных сайтов разработчиков программного обеспечения.

2.3. Используйте дополнительные средства безопасности программного обеспечения – антивирусные программы, программы защиты от спам-рассылок и пр.

Используйте только современное, лицензионное антивирусное программное обеспечение.

2.4. Если у Вас есть подозрение, что Ваш **Пароль или Логин скомпрометированы, т.е. стали известны третьим лицам**, либо произошло несанкционированное списание средств со Счета:

2.4.1. Незамедлительно выключите компьютер (ноутбук, планшет и т.п.).

2.4.2. **Если инцидент произошел в рабочее время Банка (для определения рабочего и нерабочего времени, по тексту настоящего Регламента, используется Московское время):**

Незамедлительно сообщите об инциденте по телефону Банка: +7 (495)777-11-77 или 8 (800) 777-11-77.

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении о присоединении к Договору.

После проведения аутентификации Банк незамедлительно осуществит блокировку Вашего Пароля и Идентификатора пользователя для входа в Систему ДБО, а также блокировку возможности проведения через Систему ДБО операций по Вашим счетам/картам, подключенным к Системе ДБО.

2.4.3. **Если инцидент произошел в нерабочее время Банка:**

2.4.3.1. Если к Системе ДБО подключены банковские карты, незамедлительно позвоните в Процессинговый центр для блокировки счетов банковских карт: телефон Банка, который переадресует Ваш звонок на телефон Процессингового центра: +7 (495) 777-11-79.

2.4.3.2. Незамедлительно примите меры для отзыва распоряжений на проведение расходных операций по Вашим счетам/картам, несанкционированных Вами. Для этих целей желательно использовать другой компьютер.

Следует учитывать, что через Систему ДБО распоряжение может быть отозвано Клиентом в день его регистрации в Системе ДБО и только в том случае, если оно не исполнено, и Банк имеет возможность отменить его исполнение.

В других случаях не исполненное Банком распоряжение (если Банк имеет возможность его отзыва) может быть отозвано с 9 час. 00 мин. по Вашему звонку на телефон Банка: +7 (495) 777-11-77 или 8 (800) 777-11-77.

Для проведения Банком аутентификации Вам потребуется назвать Кодовое слово, которое Вы указали в Заявлении о присоединении к Договору. После проведения аутентификации Банк незамедлительно осуществит блокировку Вашего Пароля и Идентификатора пользователя для входа в Систему ДБО, а также блокировку возможности проведения через Систему ДБО операций по Вашим счетам/картам, подключенным к Системе.

2.5. Если утерян либо похищен телефон (СИМ - карта) с номером, указанным в Заявлении о присоединении к Договору, незамедлительно сообщите об этом оператору сотовой связи для блокировки СИМ – карты.

Сообщите об инциденте в Банк по телефону +7(495)777-11-77 или 8-800-777-11-77 незамедлительно, если инцидент произошел в рабочее время Банка, либо в 9 час. первого рабочего дня Банка, если инцидент произошел в нерабочее время.

2.6. Никогда и никому не сообщайте Ваш Пароль и Одноразовый пароль, включая сотрудников Банка.

2.7. Не сохраняйте Ваш Пароль и Логин на компьютере либо на других носителях электронной информации.

2.8. Внимательно проверяйте текст sms - сообщения, которое содержит не только Одноразовый пароль, но также краткую информацию о совершаемой операции. Например, «19.02.2013 09:50:13 Ваш пароль номер 15: 0023216682 Perevod s 4081781020300006353 na 42306810300020001789».

2.9. Никогда не подтверждайте операцию Одноразовым паролем, если информация в sms - сообщении не совпадает с операцией, которую Вы хотите подтвердить.

2.10. Не устанавливайте на мобильный телефон, на который Банк отправляет sms - сообщения с Одноразовым паролем, приложения, полученные от неизвестных Вам источников. Банк никогда не рассылает своим клиентам ссылки и указания на установку приложений, за исключением

приложений, размещённых самим Банком в официальных магазинах интернет-приложений для Android и Apple. Используйте только официальные приложения банка, доступные в официальных репозиториях производителей мобильных платформ - App Store и Google Play. Обязательно убедитесь, что разработчиком указан - МОРСКОЙ БАНК (АО) (MARITIME BANK).

При получении такого предложения от Банка незамедлительно, или в 9 час. первого рабочего дня Банка, сообщите об этом по телефону: +7 (495) 777-11-77 или 8 (800) 777-11-77.

2.11. Не заходите в Систему ДБО с того же мобильного телефона, устройства, на которое приходят sms - сообщения Банка с Одноразовым паролем.

По возможности, используйте в качестве устройства для получения sms - сообщений от Банка простейший мобильный телефон, а не смартфон, поскольку риск заражения смартфона вредоносным программным обеспечением неизмеримо выше.

2.12. Не реже одного раза в день просматривайте выписки об операциях по счетам/картам, подключенным к Системе ДБО.

2.13. Для связи с Банком используйте только телефоны, указанные в настоящих Рекомендациях либо на официальном сайте в информационно – телекоммуникационной сети «Интернет» по адресу: www.maritimebank.com.

