

ИНСТРУКЦИЯ

по безопасной работе Клиента в Системе дистанционного банковского обслуживания клиентов – физических лиц (Системе ДБО ФЛ)

1. Меры безопасности при работе в Системе ДБО ФЛ:

1.1. В Системе ДБО ФЛ используются следующие механизмы защиты информации:

- многофакторная аутентификация;
- защита от автоматизированной регистрации и подбора логинов программами-роботами;
- для подтверждения документов используются одноразовые пароли.

1.2. Механизм многофакторной аутентификации позволяет максимально защититься от попыток злоумышленника получить конфиденциальную информацию, необходимую для доступа к картам и текущим счетам Клиента и предполагает наличие не менее двух факторов аутентификации из различных категорий:

- 1) то, что знает Клиент (Долговременный пароль);
- 2) то, чем обладает Клиент (источник одноразовых паролей);
- 3) то, что Банк знает о Клиенте (характеристики его Средства доступа – DeviceID).

В Системе ДБО ФЛ используются следующие механизмы безопасной аутентификации: долговременный пароль, одноразовый пароль, персональная страница, CAPTCHA, DeviceID.

1.2.1. Долговременный пароль задается Клиентом самостоятельно. В Банке долговременный пароль не генерируется работником Банка и не хранится в явном виде. Это снимает проблему дистрибуции долговременных паролей и устраняет риски компрометации долговременного пароля в Банке в процессе регистрации Клиента.

1.2.2. Для защиты от автоматизированной регистрации и подбора логинов программами-роботами используется механизм различения человека и компьютера – CAPTCHA.

Принцип отображения CAPTCHA при входе в Систему ДБО ФЛ:

1) CAPTCHA начинает отображаться после определенного числа неуспешных попыток входа – неправильного ввода комбинации «логин – пароль».

2) Включен режим Safe Mode, при котором все пользователи должны вводить CAPTCHA для входа в систему.

1.2.3. Одноразовый пароль¹ – средства подтверждения целостности и авторства формируемых и отправляемых через Систему ДБО ФЛ электронных документов (ЭД):

В качестве доказательства целостности и авторства, формируемых и отправляемых через Систему ДБО ФЛ документов, используется одноразовый пароль, передаваемый Банком в виде SMS-сообщения на указанный Клиентом и зарегистрированный в Банке Доверенный номер. Одноразовый пароль вводится Клиентом в Системе ДБО ФЛ: Клиент, после заведения в Системе ДБО ФЛ документа, нажимает «Далее». SMS-код (одноразовый пароль) состоящий из цифр поступает на Средство получения одноразовых паролей. Клиент, после заведения в Системе ДБО ФЛ документа, вводит в поле «введите SMS-код» и нажимает на соответствующую ссылку «отправить в банк». После успешного подтверждения, осуществляется проведение ЭД в Системе ДБО ФЛ.

1.2.4. Персональная страница – это страница, которая содержит индивидуальный интерфейс Клиента (индивидуальную картинку, цвета фона и рамки виртуальной клавиатуры, задаваемые Клиентом), который видит Клиент при входе в систему. Страница настраивается Клиентом самостоятельно, и при авторизации в системе позволяет удостовериться, что работа с Системой действительно происходит на странице Официального сайта Банка, а не поддельной. Для обеспечения безопасной работы Клиента при проведении финансовых операций со своими денежными средствами, Клиент должен осуществлять аутентификацию в системе только со своей персональной страницы.

Персональная картинка – часть персональной страницы Клиента. В процессе работы она может быть заменена на другое изображение. Для этого необходимо нажать кнопку «Обзор», указать путь к индивидуальной картинке.

При работе с Системой необходимо помнить о возможности фишинговых атак. В процессе фишинга используются массовые почтовые рассылки от имени популярных брендов, а также личные сообщения внутри различных сервисов, например, от имени банков. В почтовом письме может сообщаться, например, что аккаунт/банковский счет и др. будет "заморожен" до тех пор, пока вы еще раз не заполните анкету на сайте или не войдете в свой персональный раздел. При этом в письме приводится ссылка, которая ведет не на официальную страницу сервиса, а на ее точную копию. Естественно, оставленная вами информация попадает в руки мошенников. При первом входе в Систему задайте свою персональную картинку. Злоумышленник не может узнать эти данные и отобразить на своем поддельном сайте. Если вы видите свои персональные картинку и виртуальную клавиатуру –

¹ В случае (ях) направления его Банком.

значит вы находитесь на настоящем сайте Банка и можете вводить в соответствующие поля свои логин и пароль для работы в Системе.

1.2.5. В качестве второго фактора аутентификации выступает либо одноразовый пароль, либо комбинация из долговременного пароля и DeviceID. DeviceID – набор уникальных параметров, позволяющих идентифицировать рабочее место Клиента. Клиент может зарегистрировать свое рабочее место как доверенное, сохранив его DeviceID в системе. При последующих входах с того же рабочего места компьютер Клиента будет опознан по DeviceID, и для прохождения аутентификации потребуются ввести только долговременный пароль.

Описанные технологии безопасности позволяют обеспечить в Системе максимальный уровень защищенности, возможный для современных решений электронного банкинга.

2. Рекомендации по организации парольной защиты:

2.1. Клиент в обязательном порядке должен сменить Долговременный (технический) пароль при первом входе в Систему ДБО ФЛ после завершения процедуры регистрации в Системе ДБО ФЛ и получения полного доступа к услугам Системы ДБО ФЛ.

2.2. Рекомендуется периодически менять Долговременный пароль, но в обязательном порядке не реже одного раза в год.

2.3. Рекомендуется, чтобы Долговременный пароль состоял из латинских букв в разных регистрах, цифр и специальных символов. Под полем ввода Долговременного пароля расположен цветовой индикатор надежности пароля.

2.4. Необходимо выбирать Долговременный пароль с наиболее высоким уровнем надежности.

2.5. Для того чтобы Долговременный пароль был безопасным, его значение не должно совпадать с логином.

2.6. Долговременный пароль не должен состоять из одних цифр, не должен быть слишком коротким и состоять из символов, находящихся на одной линии на клавиатуре.

2.7. Долговременный пароль не должен быть значимым словом (ваше имя, дата рождения, девичья фамилия жены и т.д.), которое можно легко подобрать, или угадать.

3. Хранение информации по сформированным и проведенным документам через Систему ДБО ФЛ:

3.1. Информацию о платежах и переводах через Систему ДБО ФЛ можно получить в меню Системы ДБО ФЛ «Платежи и переводы», «История платежей и переводов в Интернет-банке».

4. Порядок восстановления Долговременного пароля, изменения Логина и

Долговременного пароля для доступа в Системе ДБО ФЛ:

4.1. После достижения определенного количества неуспешных последовательных попыток ввода паролей, происходит временная, а после и постоянная блокировка учетной записи для Системы ДБО ФЛ. При этом на Доверенный номер Клиента поступит уведомление о блокировке учетной записи и дальнейших возможных действиях.

4.2. В случае, если Клиент утратил (забыл) Долговременный пароль, то для восстановления Долговременного пароля Клиенту необходимо посетить лично (с документом, удостоверяющим личность Клиента) одно из Подразделений Банка, осуществляющих процедуры регистрации и подключения Клиентов к Системе ДБО ФЛ (перечень таких подразделений указан на Официальном сайте Банка), и оформить Заявление об изменении Доверенного номера/блокировке (разблокировке) Доверенного номера и Системы ДБО ФЛ/о восстановлении долговременного пароля/установлении лимита. После проверки и подписания Сторонами указанного заявления, Банком будет направлен на Доверенный номер Клиента SMS-сообщение с Долговременным (техническим) паролем для входа Клиента в Систему ДБО ФЛ. Долговременный (технический), пароль подлежит изменению Клиентом самостоятельно при первом входе в Систему ДБО ФЛ по данному паролю.

4.3. При возникновении у Клиента необходимости в смене Долговременного пароля, ему необходимо зайти в Систему ДБО ФЛ и перейдя по ссылкам «Настройки»/«Профиль»/«Сменить пароль» осуществить самостоятельную смену Долговременного пароля. Смена Долговременного пароля осуществляется путем ввода Клиентом старого (ранее действовавшего) Долговременного пароля и затем нового пароля (вводится дважды).

4.4. Для изменения Логина Клиенту необходимо зайти в Систему ДБО ФЛ и перейдя по ссылкам «Настройки»/«Профиль»/«Сменить Логин» осуществить самостоятельную смену Логина. Смена Логина осуществляется путем ввода нового Логина и подтверждением нового (веденного) Логина вводом действующего Долговременного пароля (вводится один раз).