Приложение 3
к Правилам электронного документооборота
Банка «СКС» (ООО) при обслуживании
клиентов на рынках ценных бумаг

Требования к реализации мер по защите информации
клиентом при работе с Личным Кабинетом

1. Требования технической защиты устройства доступа Клиента к Личному кабинету, реализуемые Клиентом.

Перед подключением к Личному кабинету должен обеспечить работу устройства в следующем режиме:

− на устройстве, с которого планируется осуществлять подключение к Личному кабинету, должны быть установлены лицензионные, регулярно обновляемые (устанавливаются обновления безопасности) операционная система, антивирусное программное обеспечение и web-браузер;

− на устройстве, с которого планируется осуществлять подключение к Личному кабинету, при наличие технической возможности должен быть настроен и использоваться локальный межсетевой экран, настроенный на работу только с необходимыми сетевыми ресурсами по поддерживаемым ими протоколам;

− устройство должно использовать процедуру аутентификации доступа к устройству прежде, чем предоставить ресурсы пользователю (требуется ввод логина и пароля).

2. Организационные меры по защите информации, реализуемые Клиентом:

− для входа в Личный кабинет требуется ввести только Логин, Пароль (Базовые Аутентификационные данные). Наличие полей для ввода иной информации (например: Номер паспорта, Ф.И.О Клиента) на главной странице означает, что Клиент попал на мошеннический сайт. О данном факте Клиент должен, прекратив работу с мошенническим сайтом, незамедлительно сообщить в Банк;

− Клиент никогда и никому не сообщает Логин, Пароль и Коды подтверждения;

− Клиент перед Аутентификацией входа должен убедиться, что в адресной строке браузера указан правильный адрес Личного кабинета(https://lk.sksbank.ru);

− Клиент убеждается, что используется защищенное SSL-соединение (отсутствуют сообщения об ошибке сертификата, в браузере изображен значок закрытого замка или рядом с адресной строкой имеется поле, индицирующее корректность SSL- соединения);

− Клиент, используя устройство, с которого получает доступ в Личный кабинет, осуществляет избирательную навигацию в сети Интернет и старается не посещать неизвестные ему сайты;

− Клиенту настоятельно не рекомендуется использование в качестве устройства доступа к Личному кабинету аппарата сотовой связи (сотового телефона, коммуникатора, смартфона, иного устройства), одновременно используемого для работы Номера телефона Клиента и получения Кодов подтверждения;

−при любых подозрениях на мошеннические web-сайты, имитирующие Личный кабинет, мошеннические SMS-сообщения или телефонные звонки, в которых неизвестные лица представляются как работники Банка, Клиент обязан обратиться в Банк по телефону, указанному на сайте Банка в сети Интернет по адресу www.sksbank.ru.