Приложение № 4
к Соглашению об электронном документообороте
между ООО ВТБ Капитал Брокер и клиентами
(депонентами) с использованием электронной подписи
(формат ГОСТ Р 34.10-2001)

Утверждено Приказом №1/02-04-2019 от 02.04.2019 г.
редакция, действующая с 17 апреля 2019 г.

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОДПИСИ, СКЗИ И СРЕДСТВ ЭП

1. **Рекомендации по проведению мероприятий, связанных с обеспечением безопасности СКЗИ и средств ЭП:**
   - Помещения, в которых размещаются рабочие места системы ЭДО, должны обеспечивать конфиденциальность проводимых работ и исключать возможность несанкционированного нахождения в них посторонних лиц.
   - Входные двери помещений, в которых размещаются рабочие места системы ЭДО, рекомендуется оборудовать замками, обеспечивающими надежное закрытие помещений в нерабочее время, окна и двери должны быть оборудованы охранной сигнализацией.
   - Рекомендуется оснастить системные блоки компьютеров с рабочими местами системы ЭДО средствами контроля вскрытия. При выявлении факта несанкционированного вскрытия системного блока работа на таком рабочем месте должна быть прекращена.
   - Необходимо обеспечить установку на компьютеры рабочих мест системы ЭДО только необходимое, лицензионное программное обеспечение. В случае обнаружения посторонних программ, нарушения целостности программного обеспечения, работа на таком рабочем месте должна быть прекращена.
   - Для работы на автоматизированном рабочем месте системы ЭДО пользователь должен иметь навыки работы на персональном компьютере, с СКЗИ и средствами ЭП.

   для Участников СЭД, являющихся юридическими лицами:
   - В организации Участника СЭД соответствующими приказами/распоряжениями должны быть назначены уполномоченные работники - Владельцы сертификатов.
   - В организации Участника СЭД должны быть разработаны нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СКЗИ и средств ЭП.
   - Для реализации мероприятий по обеспечению безопасности в организации Участника СЭД может быть соответствующим приказом/распоряжением назначено должностное лицо, ответственное за обеспечение безопасности информации и эксплуатации СКЗИ и средств ЭП.
   - Для исключения возможности создания несанкционированного (ложного) рабочего места и попытки хищения денежных средств со счета Участника системы доступ к дистрибутиву, полученному от Брокера, должен быть разрешен только должностному лицу, ответственному за обеспечение безопасности информации и эксплуатации СКЗИ и средств ЭП.

2. **Обеспечение безопасности ключевой информации:**
   - Чрезвычайно важно обеспечить доступ к ключевому носителю только владельцу Ключа ЭП. Помните, что Электронная подпись под электронным документом вырабатывается с использованием ключевого носителя, поэтому несанкционированный доступ к ключевому носителю фактически означает возможность ставить подпись от имени владельца Ключа ЭП.
   - Необходимо исключить любые возможности несанкционированного использования ключевых носителей, для хранения ключевых носителей использовать сейф или иное хранилище, обеспечивающее сохранность ключевых носителей в отсутствии владельца Ключа ЭП.
   - В случае Компрометации ключа следует немедленно прекратить его использование и любым доступным способом сообщить в УЦ о факте Компрометации ключа (утрата ключевого носителя или пароля, защищающего ключ, в том числе с последующим обнаружением, нарушения правил хранения ключевых носителей и паролей).

Безопасность использования системы ЭДО прямо зависит от выполнения вышеперечисленных требований.