Приложение №8 к Договору о порядке обмена электронными документами с использованием Системы «Клиент-Банк» (Система «iBank2»)
№ _____ от « __ » _____20 __ г.

Заполняется в обязательном порядке при заключении Договора

Обязательства Клиента по выполнению правил безопасной работы при использовании клиентской части Системы «Клиент-Банк» (Система «iBank2»)

В соответствии с Договором о порядке обмена электронными документами с использованием Системы «Клиент-Банк» (Система «iBank2») № _____ от «_____ » _____ 20 __ г., подтверждаю, что для обеспечения безопасной работы в клиентской части Системы «Клиент-Банк»

_____

(наименование КЛИЕНТА) будут соблюдаться следующие организационные меры:

1. Требования к сохранности пароля:

- пароль выбирается самостоятельно;
- если пароль записан на бумаге, то хранится в месте, недоступном для неуполномоченных лиц, рекомендуется использовать надежные металлические хранилища, оборудованные внутренними замками;
- запрещено записывать пароль на съемный носитель, монитор, клавиатуру и пр.;
- пароль должен содержать не менее 6 различных символов (буквы, цифры, большой / малый регистр);
- в качестве пароля не должны быть использованы: ИНН и другие реквизиты КЛИЕНТА, имена и фамилии, последовательности, состоящие из повторяющихся или одних цифр (в том числе номера телефонов, памятные даты, номера автомобилей и прочее, что можно связать с КЛИЕНТОМ);
- пароль обязательно меняется, если он стал известен постороннему лицу.

2. Правила хранения и использования носителей ключевой информации:

- для хранения носителей ключевой информации необходимо использовать надежные металлические хранилища, оборудованные внутренними замками, для исключения возможности негласного доступа к ним неуполномоченных лиц;
- запрещается извлекать носители с Ключами ЭП, если они не используются для работы с Системой «Клиент-Банк»;
- никогда не передавать Ключи ЭП третьим лицам для проверки работы Системы «Клиент-Банк», проверки настроек взаимодействия с БАНКОМ и т.п. При необходимости таких проверок Владелец сертификата ключа проверки ЭП должен лично подключить носитель к рабочей станции, убедиться, что пароль доступа к ключу вводится в интерфейс Системы «Клиент-Банк», и лично ввести пароль, исключая возможность его компрометации;
- запрещается передавать носители ключевой информации третьим лицам, оставлять носители ключевой информации без присмотра, а также записывать на носитель ключевой информации постороннюю информацию;
- при возникновении любых подозрений на компрометацию (копирование) секретных Ключей ЭП или компрометацию среды исполнения (наличие в компьютере вредоносных программ) - заблокировать Ключи ЭП.

3. Ограничение доступа и требования к рабочим местам, с которых осуществляется работа с Системой «Клиент-Банк»:

- право доступа предоставляется только уполномоченным лицам, непосредственно осуществляющим работу с Системой «Клиент-Банк». Исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой «Клиент-Банк»;
- запрещается установка программных средств, не предназначенных для выполнения служебных обязанностей уполномоченных лиц КЛИЕНТА, допущенных к работе с Системой «Клиент-Банк»;
- применять на рабочем месте лицензионные ПО (операционные системы, офисные пакеты и пр.), лицензионные средства антивирусной защиты, обеспечить возможность регулярного автоматического обновления антивирусных баз;
- работа с Системой «Клиент-Банк» немедленно прекращается при подозрении, что компьютер заражен, а также в случае обнаружения незарегистрированных программ или нарушения целостности операционной системы - обязательно позвонить в банк и заблокировать Ключ ЭП в порядке, предусмотренном в п. 3.8.3 Договора.

4. Соблюдение правил безопасной работы в сети интернет на рабочих местах Системы «Клиент-Банк»:

- не открывать сайт Системы «Клиент-Банк» по ссылкам (особенно баннерным или полученным через электронную почту);
- не отвечать на подозрительные письма с просьбой выслать авторизационные и другие конфиденциальные данные;
- на компьютерах, используемых для работы с Системой «Клиент-Банк», исключить посещение интернет-сайтов сомнительного содержания, загрузку и установку нелицензионного ПО и т. п.;

- не устанавливать и не сохранять подозрительные файлы, полученные из ненадежных источников, скачанные с неизвестных web-сайтов, присланные по электронной почте, полученные в телеконференциях;
- на компьютере запрещено запускать программы, полученные не из доверенных источников;
- если КЛИЕНТ эксплуатирует выделенный высокоскоростной канал доступа в сеть интернет, ограничить диапазон IP -адресов, с которых разрешён доступ к Системе «Клиент-Банк» с использованием Ключей ЭП, зарегистрированных БАНКОМ по письму, переданному КЛИЕНТОМ на бумажном носителе в БАНК.

5. Требования к сотрудникам Клиента:

- КЛИЕНТ обязан назначить Приказом уполномоченных лиц по работе с Системой «Клиент-Банк», утвердить соответствующие должностные инструкции, исключить доступ к компьютерам неуполномоченных лиц, не имеющих отношения к работе с Системой «Клиент-Банк»;
- при регистрации в Системе «Клиент-Банк» в соответствии с п. 3.7.1 Договора, руководствоваться Инструкцией по установке Системы «Клиент-Банк» (Система «iBank2») (Приложение №7 к Договору);
- каждое уполномоченное лицо, имеющее доступ к носителям ключевой информации, паролям и другой конфиденциальной информации, должно быть проинформировано об ответственности за разглашение конфиденциальной информации и подписать соответствующие обязательства;
- при обслуживании рабочей станции, на которой используется Система «Клиент-Банк», третьими лицами — обеспечивать контроль за выполняемыми ими действиями;
- при увольнении уполномоченного лица, имевшего доступ к Ключу ЭП, обязательно позвонить в БАНК и заблокировать Ключ ЭП;
- при увольнении уполномоченного лица, имевшего технический доступ к секретному Ключу ЭП, обязательно позвонить в БАНК и заблокировать Ключ ЭП;
- при увольнении уполномоченного лица, осуществлявшего обслуживание рабочей станции, используемой для работы с Системой «Клиент-Банк», принять меры для обеспечения отсутствия вредоносных программ на компьютерах.

_____

(наименование предприятия/организации)

_____ _____ _____

(наименование должности руководителя) (подпись) (фамилия и инициалы)

М.П.

Отметки Банка

Сверка подписи и оттиска печати произведена: _____/_____