Приложение № 1
к Договору № ___
от “___” _____ 20__ г.

ТРЕБОВАНИЯ
по обеспечению информационной безопасности
при работе с системой «Клиент-Банк»

1. Настоящие Требования выполняются Клиентом при подготовке к работе с системой «Клиент-Банк» и соблюдаются в процессе эксплуатации системы «Клиент-Банк».

2. Аппаратное обеспечение рабочего места Клиента

Персональная электронно-вычислительная машина (ПЭВМ) должно иметь характеристики, не ниже следующих:

- IBM PC совместимая;
- Процессор — Intel Pentium 4 1.6GHz;
- Оперативная память — 512 Mb;
- Наличие USB-порта

3. Программное обеспечение рабочего места Клиента:

- Операционная система: Microsoft Windows (не ниже 2000 SP4);
- Виртуальная Java-машина версии не ниже 1.6.

4. Следует запретить доступ к внешним Интернет-ресурсам (сайтам), непосредственно не связанным с работой системы «Клиент-Банк». Необходимо оснастить ПЭВМ актуальной системой обнаружения и блокирования попыток несанкционированного сетевого доступа к ресурсам компьютера (персональный межсетевой экран и антивирусное программное обеспечение).

4.1. Рекомендуется ограничить доступ к интернет ресурсам только Интернет-адресом ibank.doncombank.ru на TCP порты: 80, 443, 9091.

4.2. Не реже одного раза в неделю проводить полное сканирование операционной системы антивирусным программным обеспечением.

5. Запрещается использование нелицензионного программного обеспечения, как потенциального источника вредоносного программного обеспечения.

6. Доступ неуполномоченных лиц к ПЭВМ должен быть исключен как путем физической изоляции ПЭВМ, так и использованием программной (аппаратно-программной) системы разграничения доступа. При использовании системы разграничения доступа должен исключаться доступ неавторизованного пользователя, как к компонентам системы «Клиент-Банк», так и к компонентам и разделам операционной системы ПЭВМ, а также любого другого программного обеспечения.

7. Доступ неуполномоченных лиц к ключевой информации (паролям, ключам шифрования, секретным ключам ЭП, Токенов и OTP-Токенов), используемой для обеспечения функционирования системы «Клиент-Банк» должен быть исключен. Порядок хранения и использования Токенов и OTP-Токенов должен исключать возможность доступа к ним без гарантированного обнаружения факта несанкционированного доступа. Токен должен быть доступен для программного обеспечения ПЭВМ, предназначенной для работы с системой «Клиент-Банк», только в момент сеансов связи с сервером Банка.

8. Запрещается генерировать или выполнять любые действия над секретными ключами ЭП или их носителями на любых ПЭВМ, за исключением ПЭВМ Клиента – владельца ЭП, предназначенного для работы с системой «Клиент-Банк».

9. Регулярно, не реже одного раза в квартал, проводить смену пароля к ключу ЭП. Минимальная длина пароля 6 (шесть) символов, рекомендуемая – не менее 8 (восьми). Рекомендуется использовать в пароле буквы разного регистра, цифры и специальные символы (например, @&$#).

10. При наступлении следующих событий:

- утеря Токена с последующим обнаружением или без;
- обнаружение факта несанкционированного доступа к Токену;
- увольнение сотрудников, имевших доступ к Токенам;

секретные ключи Клиента считаются скомпрометированными и подлежат немедленному выводу из обращения.

11. Следующие события рассматриваются как предпосылки к возможному доступу неуполномоченных лиц к ключевой информации:

- нарушение правил хранения и использования Токенов;
- возникновение каких-либо подозрений на утечку информации;
- обнаружение нарушения целостности программного обеспечения на ПЭВМ, используемой в системе «Клиент-

Банк»

- обнаружение вредоносного программного обеспечения на ПЭВМ, используемой в системе «Клиент-Банк»;
- обнаружение нарушения целостности топологии локальной сети Клиента, временное или постоянное;
- обнаружение попыток сетевых атак на ПЭВМ, предназначенную для работы в системе «Клиент-Банк».

В данном случае также рекомендуется произвести смену секретных ключей ЭП и другой ключевой информации.

"Банк"	**"Клиент"**
_____	_____
м.п.	м.п.